



Acunetix Threat Level 4

One or more critical-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.

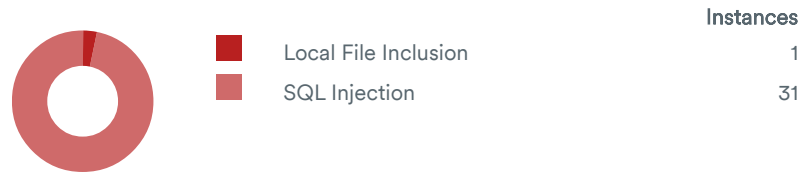
Scan Detail

Target	http://testphp.vulnweb.com/
Scan Type	Full Scan
Start Time	May 18, 2025, 12:15:44 PM GMT+6
Scan Duration	1 hour, 40 minutes
Requests	55222
Average Response Time	273ms
Maximum Response Time	20790ms
Application Build	v24.1.240111130
Authentication Profile	-

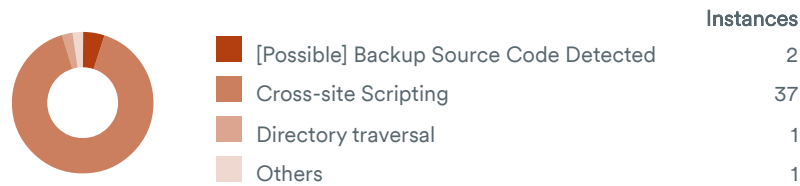
32	41	13	12	7
Critical	High	Medium	Low	Informational

Severity	Vulnerabilities	Instances
 Critical	2	32
 High	4	41
 Medium	13	13
 Low	12	12
 Informational	7	7
Total	38	105

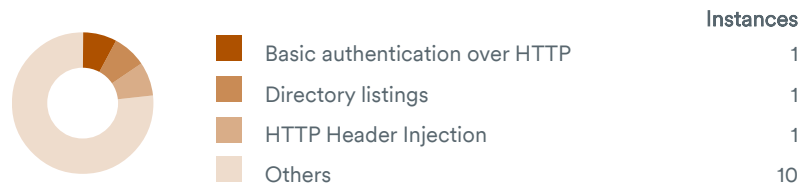
Critical Severity



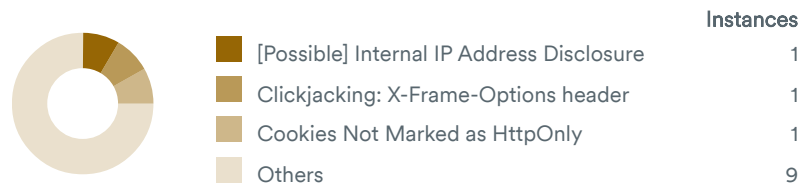
High Severity



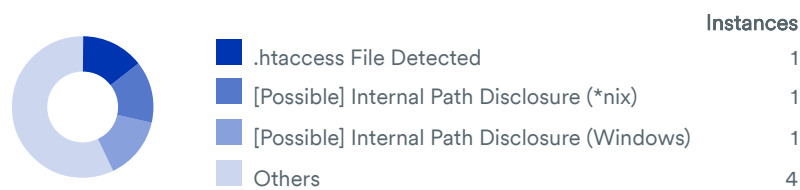
Medium Severity



Low Severity



Informational



Impacts

SEVERITY	IMPACT
 Critical	1 Local File Inclusion
 Critical	31 SQL Injection
 High	2 [Possible] Backup Source Code Detected
 High	37 Cross-site Scripting
 High	1 Directory traversal
 High	1 Possible database backup
 Medium	1 Basic authentication over HTTP
 Medium	1 Directory listings
 Medium	1 HTTP Header Injection
 Medium	1 HTTP parameter pollution
 Medium	1 Insecure crossdomain.xml policy
 Medium	1 Insecure HTTP Usage
 Medium	1 JetBrains .idea project directory
 Medium	1 Open Redirection
 Medium	1 PHP errors enabled
 Medium	1 PHP session.use_only_cookies Is Disabled
 Medium	1 PHPinfo pages
 Medium	1 SSL/TLS Not Implemented
 Medium	1 User credentials are sent in clear text
 Low	1 [Possible] Internal IP Address Disclosure
 Low	1 Clickjacking: X-Frame-Options header
 Low	1 Cookies Not Marked as HttpOnly
 Low	1 Cookies with missing, inconsistent or contradictory properties
 Low	1 PHP allow_url_fopen Is Enabled
 Low	1 PHP allow_url_fopen Is Enabled
 Low	1 PHP display_errors Is Enabled
 Low	1 PHP open_basedir Is Not Configured
 Low	1 Possible sensitive files

SEVERITY	IMPACT	
 Low	1	Possible username or password disclosure
 Low	1	Programming Error Messages
 Low	1	Version Disclosure (PHP)
 Informational	1	.htaccess File Detected
 Informational	1	[Possible] Internal Path Disclosure (*nix)
 Informational	1	[Possible] Internal Path Disclosure (Windows)
 Informational	1	[Possible] WS_FTP Log File Detected
 Informational	1	Content Security Policy (CSP) Not Implemented
 Informational	1	Generic Email Address Disclosure

Local File Inclusion

This script is possibly vulnerable to file inclusion attacks.

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

It is possible for a remote attacker to include a file from local or remote resources and/or execute arbitrary script code with the privileges of the web-server.

<http://testphp.vulnweb.com/showimage.php>

URL encoded GET input **file** was set to **showimage.php**

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"];

// restrict urls
if (filter_var($name, FILTER_VALIDATE_URL)) {
exit();
}

$fp = fopen($name, 'rb');

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

// dump the picture and stop the script
...
```

Request

```
GET /showimage.php?file=showimage.php&size=160 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Edit the source code to ensure that input is properly validated. Where is possible, it is recommended to make a list of accepted filenames and restrict the input to that list.

For PHP, the option **allow_url_fopen** would normally allow a programmer to open, include or otherwise use a remote file using a URL rather than a local file path. It is recommended to disable this option from php.ini.

References

[PHP - Using remote files](https://www.php.net/manual/en/features.remote-files.php)

<https://www.php.net/manual/en/features.remote-files.php>

[OWASP PHP Top 5](https://www.owasp.org/index.php/PHP_Top_5)

https://www.owasp.org/index.php/PHP_Top_5

[Remote file inclusion](https://en.wikipedia.org/wiki/Remote_file_inclusion)

https://en.wikipedia.org/wiki/Remote_file_inclusion

SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

Impact

An attacker can use SQL injection to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further.

<http://testphp.vulnweb.com/>



Path Fragment input `/<s/<s>-[*].html` was set to `1AcuStart028908""178247AcuEnd`

Request

```
GET /Mod_Rewrite_Shop/RateProduct-1AcuStart028908""178247AcuEnd.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/AJAX/infoartist.php>



URL encoded GET input `id` was set to `1AcuStart826360""344064AcuEnd`

Request

```
GET /AJAX/infoartist.php?id=1AcuStart826360""344064AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Accept: */*
Referer: http://testphp.vulnweb.com/
Cookie: mycookie=3
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
```

Host: testphp.vulnweb.com
Connection: Keep-alive

<http://testphp.vulnweb.com/AJAX/infocateg.php>



Verified

URL encoded GET input id was set to 1AcuStart139891'"296235AcuEnd

Request

```
GET /AJAX/infocateg.php?id=1AcuStart139891'"296235AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Accept: */*
Referer: http://testphp.vulnweb.com/
Cookie: mycookie=3
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/AJAX/infotitle.php>



Verified

URL encoded POST input id was set to 1AcuStart266685'"497093AcuEnd

Request

```
POST /AJAX/infotitle.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://testphp.vulnweb.com/
Cookie: mycookie=3
Content-Length: 32
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

id=1AcuStart266685'"497093AcuEnd
```

<http://testphp.vulnweb.com/artists.php>



Verified

URL encoded GET input artist was set to 1AcuStart430998'"561843AcuEnd

Request

```
GET /artists.php?artist=1AcuStart430998'"561843AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
```

<http://testphp.vulnweb.com/listproducts.php>



URL encoded GET input **artist** was set to **1AcuStart431020'"412366AcuEnd**

Request

```
GET /listproducts.php?artist=1AcuStart431020'"412366AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/listproducts.php>



URL encoded GET input **cat** was set to **1AcuStart681597'"981626AcuEnd**

Request

```
GET /listproducts.php?cat=1AcuStart681597'"981626AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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



URL encoded GET input **id** was set to **1AcuStart228153'"958098AcuEnd**

Request

```
GET /Mod_Rewrite_Shop/buy.php?id=1AcuStart228153'"958098AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/



Request

```
GET /Mod_Rewrite_Shop/BuyProduct-1/?id=1ACUSTART'"ACUEND HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
User-Agent: 1'"2000
referer: 1'"3000
client-ip: 1'"4000
x-forwarded-for: 1'"5000
accept-language: 1'"6000
via: 1'"7000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/



Verified

URL encoded GET input id was set to 1AcuStart608178'"714669AcuEnd

Request

```
GET /Mod_Rewrite_Shop/BuyProduct-1/?id=1AcuStart608178'"714669AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/



Verified

Request

```
GET /Mod_Rewrite_Shop/BuyProduct-2/?id=1ACUSTART'"ACUEND HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
User-Agent: 1'"2000
referer: 1'"3000
client-ip: 1'"4000
x-forwarded-for: 1'"5000
accept-language: 1'"6000
via: 1'"7000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/



Verified

URL encoded GET input id was set to 1AcuStart935058'"230167AcuEnd

Request

```
GET /Mod_Rewrite_Shop/BuyProduct-2/?id=1AcuStart935058'"230167AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/



Verified

Request

```
GET /Mod_Rewrite_Shop/BuyProduct-3/?id=1ACUSTART'"ACUEND HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
User-Agent: 1'"2000
referer: 1'"3000
client-ip: 1'"4000
x-forwarded-for: 1'"5000
accept-language: 1'"6000
via: 1'"7000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/



Verified

URL encoded GET input id was set to 1AcuStart011599'"424098AcuEnd

Request

```
GET /Mod_Rewrite_Shop/BuyProduct-3/?id=1AcuStart011599'"424098AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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



Verified

URL encoded GET input id was set to 1AcuStart292288'"242668AcuEnd

Request

```
GET /Mod_Rewrite_Shop/details.php?id=1AcuStart292288'"242668AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
```

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/

Error message found:

You have an error in your SQL syntax

Request

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/?id=1'"1000 HTTP/1.1
User-Agent: 1'"2000
referer: 1'"3000
client-ip: 1'"4000
x-forwarded-for: 1'"5000
accept-language: 1'"6000
via: 1'"7000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/



Verified

URL encoded GET input id was set to 1AcuStart424494'"619899AcuEnd

Request

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/?id=1AcuStart424494'"619899AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/



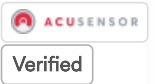
Verified

Request

```
GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/?id=1ACUSTART'"ACUEND HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
User-Agent: 1'"2000
referer: 1'"3000
client-ip: 1'"4000
x-forwarded-for: 1'"5000
```


accept-language: 1""6000
via: 1""7000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: testphp.vulnweb.com
Connection: Keep-alive

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/



URL encoded GET input id was set to 1AcuStart104212""264857AcuEnd

Request

GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/?id=1AcuStart104212""264857AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/



Request

GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/?id=1ACUSTART""ACUEND HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
User-Agent: 1""2000
referer: 1""3000
client-ip: 1""4000
x-forwarded-for: 1""5000
accept-language: 1""6000
via: 1""7000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: testphp.vulnweb.com
Connection: Keep-alive

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/



URL encoded GET input id was set to 1AcuStart003625""999207AcuEnd

Request

GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/?id=1AcuStart003625""999207AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

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



URL encoded GET input id was set to 1AcuStart217196"269482AcuEnd

Request

GET /Mod_Rewrite_Shop/rate.php?id=1AcuStart217196"269482AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html



URL encoded GET input id was set to 1AcuStart949196"329808AcuEnd

Request

GET /Mod_Rewrite_Shop/RateProduct-1.html?id=1AcuStart949196"329808AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html



URL encoded GET input id was set to 1AcuStart221834"880012AcuEnd

Request

GET /Mod_Rewrite_Shop/RateProduct-2.html?id=1AcuStart221834"880012AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html



Verified

URL encoded GET input id was set to 1AcuStart903990"135379AcuEnd

Request

```
GET /Mod_Rewrite_Shop/RateProduct-3.html?id=1AcuStart903990"135379AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/product.php>



Verified

URL encoded GET input pic was set to 1AcuStart619122"167596AcuEnd

Request

```
GET /product.php?pic=1AcuStart619122"167596AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/search.php>



Verified

URL encoded POST input searchFor was set to 1AcuStart322777"000548AcuEnd

Request

```
POST /search.php?test=query HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 49
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

goButton=&searchFor=1AcuStart322777"000548AcuEnd
```

<http://testphp.vulnweb.com/search.php>



Verified

URL encoded GET input **test** was set to **1AcuStart927440'"261872AcuEnd**

Request

```
POST /search.php?test=1AcuStart927440'"261872AcuEnd HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 23
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

goButton=&searchFor=the
```

<http://testphp.vulnweb.com/secured/newuser.php>



URL encoded POST input **uname** was set to **1AcuStart090723'"033379AcuEnd**

Request

```
POST /secured/newuser.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 196
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555&ucc=4111111111111111&uemail=testing%40example.com&upass=u]H[ww6KrA9F.x-F&upass2=u]H[ww6KrA9F.x-F&uphone=555-666-0606&urname=pHqghUme&uname=1AcuStart090723'"033379AcuEnd
```

<http://testphp.vulnweb.com/userinfo.php>



URL encoded POST input **pass** was set to **1AcuStart008630'"023660AcuEnd**

Request

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 49
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

pass=1AcuStart008630'"023660AcuEnd&uname=pHqghUme
```

<http://testphp.vulnweb.com/userinfo.php>



URL encoded POST input `uname` was set to `1AcuStart946686""803645AcuEnd`

Request

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 57
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

pass=u]H[ww6KrA9F.x-F&uname=1AcuStart946686""803645AcuEnd
```

Recommendation

Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.

References

[SQL Injection \(SQLi\) - Acunetix](https://www.acunetix.com/websitesecurity/sql-injection/)

<https://www.acunetix.com/websitesecurity/sql-injection/>

[Types of SQL Injection \(SQLi\) - Acunetix](https://www.acunetix.com/websitesecurity/sql-injection2/)

<https://www.acunetix.com/websitesecurity/sql-injection2/>

[Prevent SQL injection vulnerabilities in PHP applications and fix them - Acunetix](https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/)

<https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/>

[SQL Injection - OWASP](https://www.owasp.org/index.php/SQL_Injection)

https://www.owasp.org/index.php/SQL_Injection

[Bobby Tables: A guide to preventing SQL injection](https://bobby-tables.com/)

<https://bobby-tables.com/>

[SQL Injection Cheat Sheets - Pentestmonkey](http://pentestmonkey.net/category/cheat-sheet/sql-injection)

<http://pentestmonkey.net/category/cheat-sheet/sql-injection>

[Possible] Backup Source Code Detected

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

Impact

Backup files can contain script sources, configuration files or other sensitive information that may help an malicious user to prepare more advanced attacks.

<http://testphp.vulnweb.com/index.bak>

Confidence: 80%

This file was found using the pattern `${fileName}.bak`.

Original filename: `index.php`

Pattern found:

```
<?PHP require_once("database_connect.php"); ?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLOIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of WASP Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
<h1 id="siteName">ACUNETIX ART</h1>
<h6 id="siteInfo">TEST and Demonstration site for Acunetix Web Vulnerability Scanner</h6>
<div id="globalNav">
<a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists
</a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
<a href="guestbook.php">guestbook</a>
</div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
<h2 id="pageTitle">welcome to our page</h2>
<div class="story">
<h3>Test site for WASP.</h3>
</div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
<div id="search">
<form action="search.php" method="post">
<label>search art</label>
```

```
<input name="searchFor" type="text" size="10">
<input name="goButton" type="submit" value="go">
</form>
</div>

<div id="sectionLinks">
<ul>
<li><a href="categories.php">Browse categories</a></li>
<li><a href="artists.php">Browse artists</a></li>
<li><a href="cart.php">Your cart</a></li>
<li><a href="login.php">Signup</a></li>
<li><a href="userinfo.php">Your profile</a></li>
<li><a href="guestbook.php">Our guestbook</a></li>
<?PHP if (isset($_COOKIE["login"]))echo '<li><a href=" ../logout.php">Logout</a>'; ?></li>
</ul>
</div>

<div class="relatedLinks">
<h3>Links</h3>
<ul>
<li><a href="http://www.acunetix.com">Security art</a></li>
<li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
</ul>
</div>

<div id="advert">
<p></p>
</div>

</div>

<!--end navbar -->

<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="redir.php?r=index.php">Site
Map</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wasp@acunetix.com">Contact Us</a> |
&copy;2004
Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></html>
```

Request

```
GET /index.bak HTTP/1.1
Range: bytes=0-99999
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/index.zip>

Confidence: 80%

This file was found using the pattern `${fileName}.zip`.

Original filename: `index.php`

Request

```
GET /index.zip HTTP/1.1
Range: bytes=0-99999
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

Recommendation

Remove the file(s) if they are not required on your website. As an additional step, it is recommended to implement a security policy within your organization to disallow creation of backup files in directories accessible from the web.

References

[Testing for Old, Backup and Unreferenced Files \(OWASP-CM-006\)](#)

[https://www.owasp.org/index.php/Review_Old,_Backup_and_Unreferenced_Files_for_Sensitive_Information_\(OTG-CONFIG-004\)](https://www.owasp.org/index.php/Review_Old,_Backup_and_Unreferenced_Files_for_Sensitive_Information_(OTG-CONFIG-004))

[Security Tips for Server Configuration](#)

https://httpd.apache.org/docs/2.4/misc/security_tips.html

[Protecting Confidential Documents at Your Site](#)

<http://www.w3.org/Security/Faq/wwwsf5.html>

Cross-site Scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Impact

Malicious JavaScript has access to all the same objects as the rest of the web page, including access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user.

Furthermore, JavaScript can read and make arbitrary modifications to the contents of a page being displayed to a user. Therefore, XSS in conjunction with some clever social engineering opens up a lot of possibilities for an attacker.

<http://testphp.vulnweb.com/>

URI was set to 1<ScRiPt>iFhz(9487)</ScRiPt>

The input is reflected inside a text element.

Request

GET /404.php?1<ScRiPt>iFhz(9487)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

<http://testphp.vulnweb.com/>

Verified

Path Fragment input /<s>/<s>-[*].html was set to 3""()&%<zzz><ScRiPt >USLZ(9644)</ScRiPt>

Request

```
GET /Mod_Rewrite_Shop/RateProduct-3' " () &%25<zzz><ScRiPt%20>USLZ (9644)<%2fScRiPt>.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/AJAX/infoartist.php>

URL encoded GET input id was set to 1'"()&%<zzz><ScRiPt >gbik(9710)</ScRiPt>

Request

```
GET /AJAX/infoartist.php?id=1' " () %26%25<zzz><ScRiPt%20>gbik (9710) </ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Accept: */*
Referer: http://testphp.vulnweb.com/
Cookie: mycookie=3
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/AJAX/infocateg.php>

URL encoded GET input id was set to 1'"()&%<zzz><ScRiPt >HsT8(9736)</ScRiPt>

Request

```
GET /AJAX/infocateg.php?id=1' " () %26%25<zzz><ScRiPt%20>HsT8 (9736) </ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Accept: */*
Referer: http://testphp.vulnweb.com/
Cookie: mycookie=3
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/AJAX/infotitle.php>

URL encoded POST input id was set to 1'"()&%<zzz><ScRiPt >Luqh(9482)</ScRiPt>

Request

```
POST /AJAX/infotitle.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://testphp.vulnweb.com/
Cookie: mycookie=3
```

Content-Length: 49
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

id=1'()"&%<zzz><ScRiPt%20>Lugh(9482)</ScRiPt>

<http://testphp.vulnweb.com/AJAX/showxml.php>

Verified

Cookie input mycookie was set to 3'()"&%<zzz><ScRiPt >jgw(9216)</ScRiPt>

Request

POST /AJAX/showxml.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: https://www.google.com/search?hl=en&q=testing
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Cookie: mycookie=3'()"&%<zzz><ScRiPt%20>jgw(9216)</ScRiPt>
Content-Length: 0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: testphp.vulnweb.com
Connection: Keep-alive

<http://testphp.vulnweb.com/artists.php>

Verified

URL encoded GET input artist was set to 1'()"&%<zzz><ScRiPt >tYqK(9128)</ScRiPt>

Request

GET /artists.php?artist=1'()"&%<zzz><ScRiPt%20>tYqK(9128)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

<http://testphp.vulnweb.com/guestbook.php>

Verified

URL encoded POST input name was set to anonymous user'()"&%<zzz><ScRiPt >D4jQ(9660)</ScRiPt>

Request

POST /guestbook.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 96
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

name=anonymous%20user' '() %26%25<zzz><ScRiPt%20>D4jQ(9660)</ScRiPt>&submit=add%20message&text=555

<http://testphp.vulnweb.com/guestbook.php>

Verified

URL encoded POST input **text** was set to 555'')&%<zzz><ScRiPt >D4jQ(9880)</ScRiPt>

Request

```
POST /guestbook.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 96
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

name=anonymous%20user&submit=add%20message&text=555' '() %26%25<zzz><ScRiPt%20>D4jQ(9880)</ScRiPt>

<http://testphp.vulnweb.com/hpp/>

Verified

URL encoded GET input **pp** was set to 12'')&%<zzz><ScRiPt >u6T6(9817)</ScRiPt>

Request

```
GET /hpp/?pp=12' '() %26%25<zzz><ScRiPt%20>u6T6(9817)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/hpp/params.php>

Verified

URL encoded GET input **p** was set to 1'')&%<zzz><ScRiPt >omEu(9508)</ScRiPt>

Request

```
GET /hpp/params.php?p=1' '() %26%25<zzz><ScRiPt%20>omEu(9508)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/hpp/params.php>

Verified

URL encoded GET input **pp** was set to 12'')&%<zzz><ScRiPt >I2VG(9660)</ScRiPt>

Request

```
GET /hpp/params.php?p=valid&pp=12' " () %26%25<zzz><ScRiPt%20>I2VG(9660)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/listproducts.php>

Verified

URL encoded GET input **artist** was set to **1'"()&%<zzz><ScRiPt >54kV(9955)</ScRiPt>**

Request

```
GET /listproducts.php?artist=1' " () %26%25<zzz><ScRiPt%20>54kV(9955)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

<http://testphp.vulnweb.com/listproducts.php>

Verified

URL encoded GET input **cat** was set to **1'"()&%<zzz><ScRiPt >815A(9820)</ScRiPt>**

Request

```
GET /listproducts.php?cat=1' " () %26%25<zzz><ScRiPt%20>815A(9820)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

Verified

URL encoded GET input **id** was set to **1'"()&%<zzz><ScRiPt >lhRM(9099)</ScRiPt>**

Request

```
GET /Mod_Rewrite_Shop/buy.php?id=1' " () %26%25<zzz><ScRiPt%20>lhRM(9099)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
```

Host: testphp.vulnweb.com
Connection: Keep-alive

http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/

Verified

URL encoded GET input id was set to 1"()&%<zzz><ScRiPt >ScA9(9320)</ScRiPt>

Request

```
GET /Mod_Rewrite_Shop/BuyProduct-1/?id=1"()&%26%25<zzz><ScRiPt%20>ScA9(9320)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/

Verified

URL encoded GET input id was set to 1"()&%<zzz><ScRiPt >uqP7(9449)</ScRiPt>

Request

```
GET /Mod_Rewrite_Shop/BuyProduct-2/?id=1"()&%26%25<zzz><ScRiPt%20>uqP7(9449)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/

Verified

URL encoded GET input id was set to 1"()&%<zzz><ScRiPt >WYrB(9050)</ScRiPt>

Request

```
GET /Mod_Rewrite_Shop/BuyProduct-3/?id=1"()&%26%25<zzz><ScRiPt%20>WYrB(9050)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

Verified

URL encoded GET input id was set to 1"()&%<zzz><ScRiPt >3jeA(9430)</ScRiPt>

Request

GET /Mod_Rewrite_Shop/details.php?id=1'`() %26%25<zzz><ScRiPt%20>3jeA(9430)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ Verified

URL encoded GET input id was set to 1'`()&%<zzz><ScRiPt >luFl(9536)</ScRiPt>

Request

GET /Mod_Rewrite_Shop/Details/color-printer/3/?id=1'`() %26%25<zzz><ScRiPt%20>luFl(9536)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/ Verified

URL encoded GET input id was set to 1'`()&%<zzz><ScRiPt >rCRd(9446)</ScRiPt>

Request

GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/?id=1'`() %26%25<zzz><ScRiPt%20>rCRd(9446)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/ Verified

URL encoded GET input id was set to 1'`()&%<zzz><ScRiPt >I1T4(9794)</ScRiPt>

Request

GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/?id=1'`() %26%25<zzz><ScRiPt%20>I1T4(9794)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com

Connection: Keep-alive

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

Verified

URL encoded GET input id was set to 1"()&%<zzz><ScRiPt >NmXH(9597)</ScRiPt>

Request

```
GET /Mod_Rewrite_Shop/rate.php?id=1"() %26%25<zzz><ScRiPt%20>NmXH(9597)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html

Verified

URL encoded GET input id was set to 1"()&%<zzz><ScRiPt >BqaQ(9522)</ScRiPt>

Request

```
GET /Mod_Rewrite_Shop/RateProduct-1.html?id=1"() %26%25<zzz><ScRiPt%20>BqaQ(9522)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html

Verified

URL encoded GET input id was set to 1"()&%<zzz><ScRiPt >yu3B(9849)</ScRiPt>

Request

```
GET /Mod_Rewrite_Shop/RateProduct-2.html?id=1"() %26%25<zzz><ScRiPt%20>yu3B(9849)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html

Verified

URL encoded GET input id was set to 1"()&%<zzz><ScRiPt >OTle(9333)</ScRiPt>

Request

GET /Mod_Rewrite_Shop/RateProduct-3.html?id=1'()" %26%25<zzz><ScRiPt%20>OTle(9333)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

<http://testphp.vulnweb.com/product.php>

Verified

URL encoded GET input **pic** was set to **1'()"&%<zzz><ScRiPt >vaUI(9025)</ScRiPt>**

Request

GET /product.php?pic=1'()" %26%25<zzz><ScRiPt%20>vaUI(9025)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

<http://testphp.vulnweb.com/search.php>

Verified

URL encoded POST input **searchFor** was set to **the'()"&%<zzz><ScRiPt >iLfp(9405)</ScRiPt>**

Request

POST /search.php?test=query HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 68
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

goButton=&searchFor=the'()" %26%25<zzz><ScRiPt%20>iLfp(9405)</ScRiPt>

<http://testphp.vulnweb.com/search.php>

Verified

URL encoded GET input **test** was set to **query'()"&%<zzz><ScRiPt >iLfp(9158)</ScRiPt>**

Request

POST /search.php?test=query'()" %26%25<zzz><ScRiPt%20>iLfp(9158)</ScRiPt> HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 23

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

goButton=&searchFor=the

<http://testphp.vulnweb.com/secured/newuser.php>

Verified

URL encoded POST input **uaddress** was set to **555'()"&%<zzz><ScRiPt >d3TF(9834)</ScRiPt>**

Request

```
POST /secured/newuser.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 220
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555'()' %26%25<zzz><ScRiPt%20>d3TF(9834)
</ScRiPt>&ucc=4111111111111111&uemail=testing%40example.com&upass=u]H[ww6KrA9F.x-F&upass2=u]H[ww6KrA9F.x-F&uphone=555-666-
0606&urname=pHqghUme&uuname=pHqghUme
```

<http://testphp.vulnweb.com/secured/newuser.php>

Verified

URL encoded POST input **ucc** was set to **411111111111111'()"&%<zzz><ScRiPt >d3TF(9711)</ScRiPt>**

Request

```
POST /secured/newuser.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 220
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555&ucc=411111111111111'()' %26%25<zzz><ScRiPt%20>d3TF(9711)
</ScRiPt>&uemail=testing%40example.com&upass=u]H[ww6KrA9F.x-F&upass2=u]H[ww6KrA9F.x-F&uphone=555-666-
0606&urname=pHqghUme&uuname=pHqghUme
```

<http://testphp.vulnweb.com/secured/newuser.php>

Verified

URL encoded POST input **uemail** was set to **testing@example.com'()"&%<zzz><ScRiPt >d3TF(9388)</ScRiPt>**

Request

```
POST /secured/newuser.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
```

Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 220
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555&ucc=4111111111111111&uemail=testing%40example.com'()" %26%25<zzz><ScRiPt%20>d3TF(9388)
</ScRiPt>&upass=u]H[ww6KrA9F.x-F&upass2=u]H[ww6KrA9F.x-F&uphone=555-666-0606&urname=pHqghUme&uuname=pHqghUme

<http://testphp.vulnweb.com/secured/newuser.php>

Verified

URL encoded POST input uphone was set to 555-666-0606'()"&%<zzz><ScRiPt >d3TF(9222)</ScRiPt>

Request

POST /secured/newuser.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 220
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555&ucc=4111111111111111&uemail=testing%40example.com&upass=u]H[ww6KrA9F.x-F&upass2=u]H[ww6KrA9F.x-F&uphone=555-666-0606'()" %26%25<zzz><ScRiPt%20>d3TF(9222)</ScRiPt>&urname=pHqghUme&uuname=pHqghUme

<http://testphp.vulnweb.com/secured/newuser.php>

Verified

URL encoded POST input urname was set to pHqghUme'()"&%<zzz><ScRiPt >d3TF(9688)</ScRiPt>

Request

POST /secured/newuser.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 220
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555&ucc=4111111111111111&uemail=testing%40example.com&upass=u]H[ww6KrA9F.x-F&upass2=u]H[ww6KrA9F.x-F&uphone=555-666-0606&urname=pHqghUme'()" %26%25<zzz><ScRiPt%20>d3TF(9688)</ScRiPt>&uuname=pHqghUme

<http://testphp.vulnweb.com/secured/newuser.php>

Verified

URL encoded POST input uuname was set to pHqghUme'()"&%<zzz><ScRiPt >d3TF(9012)</ScRiPt>

Request

POST /secured/newuser.php HTTP/1.1
Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 220
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555&ucc=4111111111111111&uemail=testing%40example.com&upass=u]H[ww6KrA9F.x-F&upass2=u]H[ww6KrA9F.x-F&uphone=555-666-0606&urname=pHqghUme&uname=pHqghUme'"()%26%25<zzz><ScRiPt%20>d3TF(9012)</ScRiPt>

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

Verified

URL encoded POST input **pass** was set to u]H[ww6KrA9F.x-F'"()%&%<zzz><ScRiPt >mIQb(9539)</ScRiPt>

Request

POST /userinfo.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 81
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

pass=u]H[ww6KrA9F.x-F'"()%26%25<zzz><ScRiPt%20>mIQb(9539)</ScRiPt>&uname=pHqghUme

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

Verified

URL encoded POST input **uname** was set to pHqghUme'"()%&%<zzz><ScRiPt >mIQb(9331)</ScRiPt>

Request

POST /userinfo.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 81
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

pass=u]H[ww6KrA9F.x-F&uname=pHqghUme'"()%26%25<zzz><ScRiPt%20>mIQb(9331)</ScRiPt>

Recommendation

Apply context-dependent encoding and/or validation to user input rendered on a page

References

[Cross-site Scripting \(XSS\) Attack - Acunetix](#)
<https://www.acunetix.com/websitesecurity/cross-site-scripting/>

[Types of XSS - Acunetix](#)

<https://www.acunetix.com/websitesecurity/xss/>

[XSS Filter Evasion Cheat Sheet](#)

https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

[Excess XSS, a comprehensive tutorial on cross-site scripting](#)

<https://excess-xss.com/>

[Cross site scripting](#)

https://en.wikipedia.org/wiki/Cross-site_scripting

Directory traversal

This script is possibly vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files 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.

<http://testphp.vulnweb.com/showimage.php>



Verified

URL encoded GET input file was set to 1018811/../../../../xxx\...\764125

Request

```
GET /showimage.php?file=1018811/../../../../xxx%5C..%5C..%5C764125&size=160 HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Your script should filter metacharacters from user input.

References

[Acunetix Directory Traversal Attacks](#)

<https://www.acunetix.com/websitesecurity/directory-traversal/>

Possible database backup

Manual confirmation is required for this alert.

One or more possible database backups were identified. A database backup contains a record of the table structure and/or the data from a database and is usually in the form of a list of SQL statements. A database backup is most often used for backing up a database so that its contents can be restored in the event of data loss. This information is highly sensitive and should never be found on a production system.

Impact

These file(s) may disclose sensitive information. This information can be used to launch further attacks.

<http://testphp.vulnweb.com/admin/create.sql>

Pages with possible database backups:

-

Request

```
GET /admin/create.sql HTTP/1.1
Range: bytes=0-99999
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Sensitive files such as database backups should never be stored in a directory that is accessible to the web server. As a workaround, you could restrict access to these file(s).

Basic authentication over HTTP

In the context of an HTTP transaction, basic access authentication is a method for an HTTP user agent to provide a user name and password when making a request.

One or more directories are protected using Basic Authentication over an HTTP connection. With Basic Authentication the user credentials are sent as cleartext and because HTTPS is not used, they are vulnerable to packet sniffing.

Impact

User credentials are sent as cleartext and are vulnerable to packet sniffing.

<http://testphp.vulnweb.com/>

Verified

Pages with basic authentication over HTTP:

- <http://testphp.vulnweb.com/clearguestbook.php>

Request

```
GET /clearguestbook.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
```

Host: testphp.vulnweb.com
Connection: Keep-alive

Recommendation

Use Basic Authentication over an HTTPS connection.

References

[Basic access authentication](https://en.wikipedia.org/wiki/Basic_access_authentication)

https://en.wikipedia.org/wiki/Basic_access_authentication

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://testphp.vulnweb.com/>

Verified

Folders with directory listing enabled:

- <http://testphp.vulnweb.com/wvstests/>
- http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/
- http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/
- <http://testphp.vulnweb.com/.idea/>
- <http://testphp.vulnweb.com/.idea/scopes/>
- <http://testphp.vulnweb.com/Flash/>
- <http://testphp.vulnweb.com/CVS/>
- <http://testphp.vulnweb.com/Connections/>
- <http://testphp.vulnweb.com/Templates/>
- http://testphp.vulnweb.com/_mmServerScripts/
- <http://testphp.vulnweb.com/admin/>
- <http://testphp.vulnweb.com/pictures/>
- <http://testphp.vulnweb.com/vendor/>
- <http://testphp.vulnweb.com/images/>
- http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/

Request

```
GET /wvstests/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

[CWE-548: Exposure of Information Through Directory Listing](https://cwe.mitre.org/data/definitions/548.html)
https://cwe.mitre.org/data/definitions/548.html

HTTP Header Injection

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.

<http://testphp.vulnweb.com/redir.php>  Verified

URL encoded GET input r was set to ACUSTART ACUEND

Request

```
GET /redir.php?r=ACUSTART%0D%0AACUEND HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

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

References

[Acunetix CRLF Injection Attack](https://www.acunetix.com/websitesecurity/crlf-injection/)

<https://www.acunetix.com/websitesecurity/crlf-injection/>

[Whitepaper - HTTP Response Splitting](https://packetstormsecurity.com/papers/general/whitepaper_httpresponse.pdf)

https://packetstormsecurity.com/papers/general/whitepaper_httpresponse.pdf

[Introduction to HTTP Response Splitting](https://web.archive.org/web/20210507213818/https://securiteam.com/securityreviews/5wp0e2kfgk/)

<https://web.archive.org/web/20210507213818/https://securiteam.com/securityreviews/5wp0e2kfgk/>

HTTP parameter pollution

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

<http://testphp.vulnweb.com/hpp/>

URL encoded GET input pp was set to 12&n911727=v944330

Parameter precedence: last occurrence

Affected link: [params.php?p=valid&pp=12&n911727=v944330](http://testphp.vulnweb.com/params.php?p=valid&pp=12&n911727=v944330)

Affected parameter: p=valid

Request

```
GET /hpp/?pp=12%26n911727=v944330 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

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

References

[HTTP Parameter Pollution](#)

Insecure crossdomain.xml policy

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="*" />
<allow-http-request-headers-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.

<http://testphp.vulnweb.com/crossdomain.xml>

The following issues were detected:

- **/crossdomain.xml:** Element "allow-access-from" has attribute "domain" set to "*"
- **/crossdomain.xml:** Element "allow-access-from" has attribute "secure" set to "false"

Request

```
GET / HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: filelist;aspectalerts;packages
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Carefully evaluate which sites will be allowed to make cross-domain calls. Consider network topology and any authentication mechanisms that will be affected by the configuration or implementation of the cross-domain policy.

References

[Cross-domain policy files](#)

https://web.archive.org/web/20120303231120/http://blogs.adobe.com/stateofsecurity/2007/07/crossdomain_policy_files_1.html

Insecure HTTP Usage

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

<http://testphp.vulnweb.com/>

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

[HTTP Redirections](#)

https://infosec.mozilla.org/guidelines/web_security#http-redirections

JetBrains .idea project directory

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

Impact

These files may expose sensitive information that may help an malicious user to prepare more advanced attacks.

<http://testphp.vulnweb.com/>

workspace.xml project file found at : /.idea/workspace.xml

Pattern found:

```
<project version="4">
```

Request

```
GET /.idea/workspace.xml HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Remove these files from production systems or restrict access to the .idea directory. To deny access to all the .idea folders you need to add the following lines in the appropriate context (either global config, or vhost/directory, or from .htaccess):

```
<Directory ~ /\.idea">
Order allow,deny
Deny from all
</Directory>
```

References

[Apache Tips & Tricks: Deny access to some folders](http://www.ducea.com/2006/08/11/apache-tips-tricks-deny-access-to-some-folders/)

<http://www.ducea.com/2006/08/11/apache-tips-tricks-deny-access-to-some-folders/>

Open Redirection

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.

<http://testphp.vulnweb.com/redir.php>

URL encoded GET input r was set to <http://xfs.bxss.me?vulnweb.com>

Request

```
GET /redir.php?r=http://xfs.bxss.me%3Fvulnweb.com HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
```

Recommendation

Your script should properly sanitize user input.

References

[Unvalidated Redirects and Forwards Cheat Sheet](https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html)

https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html

[HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics](https://packetstormsecurity.com/papers/general/whitepaper_httpresponse.pdf)

https://packetstormsecurity.com/papers/general/whitepaper_httpresponse.pdf

PHP errors enabled

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix AcuSensor found that the PHP `display_errors` directive is enabled.

Impact

Application error messages may disclose sensitive information which can be used to escalate attacks.

<http://testphp.vulnweb.com/>



Verified

Current setting is : `display_errors = 1`

Observed on /

Recommendation

Adjust `php.ini` or `.htaccess` (`mod_php` with Apache HTTP Server) to disable `display_errors` (refer to 'Detailed information' section).

References

[PHP Runtime Configuration \(display_errors\)](https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

[PHP Runtime Configuration \(log_errors\)](https://www.php.net/manual/en/errorfunc.configuration.php#ini.log-errors)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.log-errors>

PHP session.use_only_cookies Is Disabled

When `use_only_cookies` is disabled, PHP will pass the session ID via the URL. This makes the application more vulnerable to session hijacking attacks. Session hijacking is basically a form of identity theft wherein a hacker impersonates a legitimate user by stealing his session ID. When the session token is transmitted in a cookie, and the request is made on a secure channel (that is, it uses SSL), the token is secure.

Impact

Application dependant - possible session hijacking.

<http://testphp.vulnweb.com/secured/phpinfo.php>

Verified

This vulnerability was detected using the information from phpinfo() page.

session.use_only_cookies: On

Request

```
GET /secured/phpinfo.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

You can enabled session.use_only_cookies from php.ini or .htaccess.

php.ini

session.use_only_cookies = 'on'

.htaccess

php_flag session.use_only_cookies on

References

[Runtime Configuration](https://www.php.net/session.configuration)

<https://www.php.net/session.configuration>

PHPinfo pages

One or more **phpinfo()** pages were found. The **phpinfo()** function exposes a large amount of information about the PHP configuration and that of its environment. This includes information about PHP compilation options and extensions, the PHP version, server information, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

Impact

The phpinfo() pages may expose sensitive information that may help an malicious user to prepare more advanced attacks.

<http://testphp.vulnweb.com/>

Confidence: 95%

PHPinfo pages found:

- /secured/phpinfo.php
- <title>phpinfo()</title>

Request

```
GET /secured/phpinfo.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

Recommendation

Remove either the call to the `phpinfo()` function from the file(s), or the file(s) itself.

References

[PHP phpinfo](#)

<https://www.php.net/manual/en/function.phpinfo.php>

SSL/TLS Not Implemented

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

Impact

Possible information disclosure.

<http://testphp.vulnweb.com/>

Verified

Request

GET / HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

User credentials are sent in clear text

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.

<http://testphp.vulnweb.com/>

Forms with credentials sent in clear text:

- <http://testphp.vulnweb.com/login.php>

```
Form name: loginform
Form action: userinfo.php
Form method: POST
Password input: pass
```

- <http://testphp.vulnweb.com/signup.php>

```
Form name: form1
Form action: /secured/newuser.php
Form method: POST
Password input: upass
```

Request

```
GET /login.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

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

[Possible] Internal IP Address Disclosure

One or more strings matching an internal IPv4 address were found. These IPv4 addresses may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

The significance of this finding should be confirmed manually.

Impact

Possible sensitive information disclosure.

<http://testphp.vulnweb.com/>

Pages with internal IPs:

- <http://testphp.vulnweb.com/404.php>
192.168.0.28
- <http://testphp.vulnweb.com/secured/phpinfo.php>
192.168.0.5

- <http://testphp.vulnweb.com/pictures/ipaddresses.txt>
192.168.0.26

Request

```
GET /404.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

Clickjacking: X-Frame-Options header

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 did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, 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 untrusted sites.

Impact

The impact depends on the affected web application.

<http://testphp.vulnweb.com/>

Paths without secure XFO header:

- <http://testphp.vulnweb.com/>
- <http://testphp.vulnweb.com/AJAX/index.php>
- <http://testphp.vulnweb.com/search.php>
- <http://testphp.vulnweb.com/AJAX/showxml.php>
- http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/version.php
- <http://testphp.vulnweb.com/artists.php>
- <http://testphp.vulnweb.com/listproducts.php>
- <http://testphp.vulnweb.com/bxss/adminPan3l/index.php>
- <http://testphp.vulnweb.com/product.php>

- <http://testphp.vulnweb.com/comment.php>
- <http://testphp.vulnweb.com/cart.php>
- http://testphp.vulnweb.com/Connections/DB_Connection.php
- http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
- http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php
- <http://testphp.vulnweb.com/hpp/params.php>
- http://testphp.vulnweb.com/secured/database_connect.php
- <http://testphp.vulnweb.com/categories.php>
- <http://testphp.vulnweb.com/disclaimer.php>
- <http://testphp.vulnweb.com/guestbook.php>
- <http://testphp.vulnweb.com/index.php>
- <http://testphp.vulnweb.com/login.php>

Request

```
GET / HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

[The X-Frame-Options response header](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

[Clickjacking](https://en.wikipedia.org/wiki/Clickjacking)

<https://en.wikipedia.org/wiki/Clickjacking>

[OWASP Clickjacking](https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)

https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

[Frame Buster Buster](https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

<https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed>

Cookies Not Marked as HttpOnly

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

Cookies can be accessed by client-side scripts.

<http://testphp.vulnweb.com/>

Verified

Cookies without HttpOnly flag set:

- <http://testphp.vulnweb.com/logout.php>

```
Set-Cookie: login=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0
```

Request

```
GET /logout.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Cookies with missing, inconsistent or contradictory properties

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, or with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

<http://testphp.vulnweb.com/>

Verified

List of cookies with missing, inconsistent or contradictory properties:

- <http://testphp.vulnweb.com/logout.php>

Cookie was set with:

```
Set-Cookie: login=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

Request

```
GET /logout.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

[MDN | Set-Cookie](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie>

[Securing cookies with cookie prefixes](https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/)

<https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/>

[Cookies: HTTP State Management Mechanism](https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05)

<https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05>

[SameSite Updates - The Chromium Projects](https://www.chromium.org/updates/same-site)

<https://www.chromium.org/updates/same-site>

[draft-west-first-party-cookies-07: Same-site Cookies](https://tools.ietf.org/html/draft-west-first-party-cookies-07)

<https://tools.ietf.org/html/draft-west-first-party-cookies-07>

PHP allow_url_fopen Is Enabled

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

Impact

Application dependant - possible remote file inclusion.

<http://testphp.vulnweb.com/>



Verified

Current setting is : `allow_url_fopen = on`

Observed on /

Recommendation

You can disable `allow_url_fopen` from either `php.ini` (for PHP versions newer than 4.3.4) or `.htaccess` (for PHP versions up to 4.3.4).

php.ini

`allow_url_fopen = 'off'`

.htaccess

`php_flag allow_url_fopen off`

References

[Runtime Configuration](#)

<https://www.php.net/manual/en/filesystem.configuration.php>

PHP allow_url_fopen Is Enabled

The PHP configuration directive `allow_url_fopen` is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling `allow_url_fopen` and bad input filtering.

`allow_url_fopen` is enabled by default.

Impact

Application dependant - possible remote file inclusion.

<http://testphp.vulnweb.com/secured/phpinfo.php>

Verified

This vulnerability was detected using the information from `phpinfo()` page.

`allow_url_fopen`: On

Request

```
GET /secured/phpinfo.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

You can disable `allow_url_fopen` from either `php.ini` (for PHP versions newer than 4.3.4) or `.htaccess` (for PHP versions up to 4.3.4).

php.ini

`allow_url_fopen = 'off'`

.htaccess

`php_flag allow_url_fopen off`

References

[Runtime Configuration](https://www.php.net/manual/en/filesystem.configuration.php)

<https://www.php.net/manual/en/filesystem.configuration.php>

PHP `display_errors` Is Enabled

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found that the PHP `display_errors` directive is enabled.

Impact

Application error messages may disclose sensitive information which can be used to escalate attacks.

<http://testphp.vulnweb.com/secured/phpinfo.php>

Verified

This vulnerability was detected using the information from `phpinfo()` page.

`display_errors`: On

Request

```
GET /secured/phpinfo.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Adjust `php.ini` or `.htaccess` (`mod_php` with Apache HTTP Server) to disable `display_errors` (refer to 'Detailed information' section).

References

[PHP Runtime Configuration \(`display\_errors`\)](https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

[PHP Runtime Configuration \(`log\_errors`\)](https://www.php.net/manual/en/errorfunc.configuration.php#ini.log-errors)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.log-errors>

PHP open_basedir Is Not Configured

The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

Impact

Application dependant - possible remote code inclusion.

<http://testphp.vulnweb.com/secured/phpinfo.php>

Verified

This vulnerability was detected using the information from phpinfo() page.

open_basedir: no value

Request

```
GET /secured/phpinfo.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

You can set open_basedir from php.ini

php.ini

open_basedir = your_application_directory

References

[Description of core php.ini directives](https://www.php.net/ini.core)

<https://www.php.net/ini.core>

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://testphp.vulnweb.com/>

Possible sensitive files:

- <http://testphp.vulnweb.com/hpp/test.php>

Request

```
GET /hpp/test.php HTTP/1.1
Accept: pcouifpj/zelk
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Restrict access to this file or remove it from the website.

References

[Web Server Security and Database Server Security](https://www.acunetix.com/websitesecurity/webserver-security/)

<https://www.acunetix.com/websitesecurity/webserver-security/>

Possible username or password disclosure

One or more credential pairs (username+password) were found. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

<http://testphp.vulnweb.com/>

Pages containing credentials:

- <http://testphp.vulnweb.com/pictures/credentials.txt>

```
username=test
password=something
```

Request

```
GET /pictures/credentials.txt HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Remove these file(s) from your website or change its permissions to remove access.

Programming Error Messages

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

These messages may also contain the location of the file that produced an unhandled exception.

Consult the 'Attack details' section for more information about the affected page(s).

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

<http://testphp.vulnweb.com/>

Application error messages:

- <http://testphp.vulnweb.com/search.php>
You have an error in your SQL syntax
- <http://testphp.vulnweb.com/showimage.php>
Warning: fopen(): Filename cannot be empty in /hj/var/www/showimage.php on line 31
- <http://testphp.vulnweb.com/artists.php>
You have an error in your SQL syntax
- <http://testphp.vulnweb.com/listproducts.php>
You have an error in your SQL syntax
- <http://testphp.vulnweb.com/bxss/adminPan3l/index.php>
Warning: mysql_connect(): Access denied for user 'bxss'@'localhost' (using password: YES) in
/hj/var/www/bxss/adminPan3l/index.php on line 2

- <http://testphp.vulnweb.com/product.php>
You have an error in your SQL syntax
- http://testphp.vulnweb.com/Connections/DB_Connection.php
Fatal error
- http://testphp.vulnweb.com/Connections/DB_Connection.php
Warning: mysql_pconnect(): Access denied for user 'root'@'localhost' in /hj/var/www/Connections/DB_Connection.php
on line 9

- http://testphp.vulnweb.com/secured/database_connect.php
Warning: mysql_connect(): Access denied for user 'wauuser'@'localhost' (using password: YES) in
/hj/var/www/secured/database_connect.php on line 2

- <http://testphp.vulnweb.com/userinfo.php>
You have an error in your SQL syntax

- <http://testphp.vulnweb.com/secured/newuser.php>
You have an error in your SQL syntax
- <http://testphp.vulnweb.com/AJAX/infoartist.php>
You have an error in your SQL syntax
- http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php
You have an error in your SQL syntax
- <http://testphp.vulnweb.com/AJAX/infotitle.php>
You have an error in your SQL syntax
- <http://testphp.vulnweb.com/bxss/cleanDatabase.php>
Warning: mysql_connect(): Access denied for user 'bxss'@'localhost' (using password: YES) in /hj/var/www/bxss/cleanDatabase.php on line 2

- <http://testphp.vulnweb.com/pictures/path-disclosure-unix.html>
Warning: Sablotron error on line 1: XML parser error 3: no element found in /usr/local/etc/httpd/htdocs2/destination-ce/destinationce/system/class/xsltTransform.class.php on line 70

- <http://testphp.vulnweb.com/bxss/vuln.php>
Warning: mysql_connect(): Access denied for user 'bxss'@'localhost' (using password: YES) in /hj/var/www/bxss/vuln.php on line 2

- <http://testphp.vulnweb.com/showimage.php>
Warning: fopen(): Filename cannot be empty in /hj/var/www/showimage.php on line 13
- <http://testphp.vulnweb.com/listproducts.php>
Warning: mysql_fetch_array() expects parameter 1 to be resource, null given in /hj/var/www/listproducts.php on line 89

- http://testphp.vulnweb.com/bxss/database_connect.php
Warning: mysql_connect(): Access denied for user 'bxss'@'localhost' (using password: YES) in /hj/var/www/bxss/database_connect.php on line 2

- http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
You have an error in your SQL syntax

Request

```
POST /search.php?test=12345'"'\");|]*%00{%0d%0a<%00>%bf%27' HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Content-Length: 23
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

goButton=&searchFor=the
```

Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

[PHP Runtime Configuration](#)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

[Improper Error Handling](#)

https://www.owasp.org/index.php/Improper_Error_Handling

Version Disclosure (PHP)

The web server is sending the X-Powered-By: response headers, revealing the PHP version.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

<http://testphp.vulnweb.com/>

Version detected: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.

Recommendation

Configure your web server to prevent information leakage from its HTTP response.

References

[PHP Documentation: header_remove\(\)](#)

<https://www.php.net/manual/en/function.header-remove.php>

[PHP Documentation: php.ini directive expose_php](#)

<https://www.php.net/manual/en/ini.core.php#ini.expose-php>

.htaccess File Detected

This directory contains an **.htaccess** file that is readable. This may indicate a server misconfiguration. htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

Impact

Possible sensitive information disclosure.

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

Verified

Request

```
GET /Mod_Rewrite_Shop/.htaccess HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Restrict access to the .htaccess file by adjusting the web server configuration.

[Possible] Internal Path Disclosure (*nix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

<http://testphp.vulnweb.com/>

Pages with paths being disclosed:

- <http://testphp.vulnweb.com/pictures/path-disclosure-unix.html>
>/usr/local/etc/httpd/htdocs2/destination
- <http://testphp.vulnweb.com/secured/phpinfo.php>
:/usr/obj/usr/src/sys/GENERIC

Request

```
GET /pictures/path-disclosure-unix.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

[Full Path Disclosure](https://www.owasp.org/index.php/Full_Path_Disclosure)

https://www.owasp.org/index.php/Full_Path_Disclosure

[Possible] Internal Path Disclosure (Windows)

One or more fully qualified path names were been found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

<http://testphp.vulnweb.com/>

Pages with paths being disclosed:

- <http://testphp.vulnweb.com/pictures/path-disclosure-win.html>
C:\inetpub\wwwroot\comparatii.php

Request

```
GET /pictures/path-disclosure-win.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

[Full Path Disclosure](https://www.owasp.org/index.php/Full_Path_Disclosure)

https://www.owasp.org/index.php/Full_Path_Disclosure

[Possible] WS_FTP Log File Detected

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

Impact

This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.

http://testphp.vulnweb.com/pictures/WS_FTP.LOG

Verified

Pattern found:

103.05.06 13:17

Request

```
GET /pictures/WS_FTP.LOG HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Remove this file from your website or change its permissions to remove access.

References

[ws_ftp.log](https://seclists.org/fulldisclosure/2004/Aug/703)

<https://seclists.org/fulldisclosure/2004/Aug/703>

Content Security Policy (CSP) Not Implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

<http://testphp.vulnweb.com/>

Paths without CSP header:

- <http://testphp.vulnweb.com/>
- <http://testphp.vulnweb.com/AJAX/index.php>
- http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/version.php
- <http://testphp.vulnweb.com/artists.php>
- <http://testphp.vulnweb.com/listproducts.php>

- <http://testphp.vulnweb.com/bxss/adminPan3l/index.php>
- <http://testphp.vulnweb.com/product.php>
- <http://testphp.vulnweb.com/comment.php>
- http://testphp.vulnweb.com/Connections/DB_Connection.php
- http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
- http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php
- <http://testphp.vulnweb.com/hpp/params.php>
- http://testphp.vulnweb.com/secured/database_connect.php
- <http://testphp.vulnweb.com/categories.php>
- <http://testphp.vulnweb.com/disclaimer.php>
- <http://testphp.vulnweb.com/guestbook.php>
- <http://testphp.vulnweb.com/index.php>
- <http://testphp.vulnweb.com/login.php>
- <http://testphp.vulnweb.com/privacy.php>
- <http://testphp.vulnweb.com/signup.php>
- <http://testphp.vulnweb.com/images/>

Request

```
GET / HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

[Implementing Content Security Policy](https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

Generic Email Address Disclosure

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

<http://testphp.vulnweb.com/>

Emails found:

- <http://testphp.vulnweb.com/>
wvs@acunetix.com
- <http://testphp.vulnweb.com/search.php>
wvs@acunetix.com
- <http://testphp.vulnweb.com/artists.php>
wvs@acunetix.com
- <http://testphp.vulnweb.com/listproducts.php>
wvs@acunetix.com
- <http://testphp.vulnweb.com/product.php>
wvs@acunetix.com
- <http://testphp.vulnweb.com/cart.php>
wvs@acunetix.com
- http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
wvs@acunetix.com
- <http://testphp.vulnweb.com/categories.php>
wvs@acunetix.com
- <http://testphp.vulnweb.com/disclaimer.php>
wvs@acunetix.com
- <http://testphp.vulnweb.com/guestbook.php>
wvs@acunetix.com
- <http://testphp.vulnweb.com/index.php>
wvs@acunetix.com
- <http://testphp.vulnweb.com/login.php>
wvs@acunetix.com

- <http://testphp.vulnweb.com/signup.php>
wvs@acunetix.com
- <http://testphp.vulnweb.com/404.php>
wvs@acunetix.com
- <http://testphp.vulnweb.com/logout.php>
wvs@acunetix.com

Request

```
GET / HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: filelist;aspectalerts;packages
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](https://en.wikipedia.org/wiki/Anti-spam_techniques)

https://en.wikipedia.org/wiki/Anti-spam_techniques

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

<http://testphp.vulnweb.com/>

Locations without Permissions-Policy header:

- <http://testphp.vulnweb.com/>
- <http://testphp.vulnweb.com/search.php>
- <http://testphp.vulnweb.com/AJAX/index.php>
- <http://testphp.vulnweb.com/AJAX/showxml.php>
- http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/version.php
- <http://testphp.vulnweb.com/artists.php>
- <http://testphp.vulnweb.com/listproducts.php>
- <http://testphp.vulnweb.com/bxss/adminPan3l/index.php>
- <http://testphp.vulnweb.com/product.php>
- <http://testphp.vulnweb.com/comment.php>
- <http://testphp.vulnweb.com/cart.php>
- http://testphp.vulnweb.com/Connections/DB_Connection.php
- http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
- http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php
- <http://testphp.vulnweb.com/hpp/params.php>
- http://testphp.vulnweb.com/secured/database_connect.php

- <http://testphp.vulnweb.com/categories.php>
- <http://testphp.vulnweb.com/disclaimer.php>
- <http://testphp.vulnweb.com/guestbook.php>
- <http://testphp.vulnweb.com/index.php>
- <http://testphp.vulnweb.com/login.php>

Request

```
GET / HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 6591335967001319549
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

References

[Permissions-Policy / Feature-Policy \(MDN\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

[Permissions Policy \(W3C\)](#)

<https://www.w3.org/TR/permissions-policy-1/>

Coverage

Ⓛ http://testphp.vulnweb.com

Ⓛ _mmServerScripts

📄 MMHTTPDB.php

📄 mysql.php

Ⓛ .idea

Ⓛ scopes

📄 scope_settings.xml

📄 .name

📄 acuart.iml

📄 encodings.xml

📄 misc.xml

📄 modules.xml

📄 vcs.xml

📄 workspace.xml

Ⓛ admin

📄 create.sql

Ⓛ AJAX

📄 artists.php

📄 categories.php

📄 htaccess.conf

📄 index.php

📄 infoartist.php

📄 infocateg.php

📄 infotitle.php

📄 showxml.php

📄 styles.css

📄 titles.php

Ⓛ bxss

Ⓛ adminPan3l

📄 index.php

📄 style.css

📄 cleanDatabase.php

📄 database_connect.php

📄 index.php

📄 test.js

📄 vuln.php

Ⓛ Connections

📄 DB_Connection.php

Ⓛ CVS

 Entries
 Entries.Log
 Repository
 Root
 Flash
 add.swf
 hpp
 index.php
 params.php
 test.php
 images
 medias
 css
 main.css
 img
 js
 common_functions.js
 Mod_Rewrite_Shop
 BuyProduct-1
 BuyProduct-2
 BuyProduct-3
 Details
 color-printer
 3
 network-attached-storage-dlink
 1
 web-camera-a4tech
 2
 images
 .htaccess
 buy.php
 details.php
 index.php
 rate.php
 RateProduct-1.html
 RateProduct-2.html
 RateProduct-3.html
 pictures
 1.jpg.tn
 2.jpg.tn
 3.jpg.tn
 4.jpg.tn

 5.jpg.tn
 6.jpg.tn
 7.jpg.tn
 8.jpg.tn
 credentials.txt
 ipaddresses.txt
 path-disclosure-unix.html
 path-disclosure-win.html
 wp-config.bak
 WS_FTP.LOG
 secured
 office_files
 filelist.xml
 database_connect.php
 index.php
 newuser.php
 office.htm
 phpinfo.php
 style.css
 Templates
 main_dynamic_template.dwt.php
 vendor
 installed.json
 wvstests
 pmwiki_2_1_19
 scripts
 version.php
 404.php
 artists.php
 cart.php
 categories.php
 clearguestbook.php
 clientaccesspolicy.xml
 comment.php
 crossdomain.xml
 database_connect.php
 disclaimer.php
 guestbook.php
 index.bak
 index.php
 index.zip
 listproducts.php

 login.php logout.php privacy.php product.php redir.php search.php sendcommand.php showimage.php signup.php style.css userinfo.php