ZAP by Checkmarx Scanning Report

Generated with ZAP on Tue 24 Jun 2025, at 19:35:36

ZAP Version: 2.16.1

ZAP by Checkmarx

Contents

About This Report

Report Description

ZAP automated scan results for DVWA testing environment.

Report Parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- http://localhost

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Summaries

Alert Counts by Risk and Confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	2 (18.2%)	2 (18.2%)	0 (0.0%)	4 (36.4%)
	Low	0 (0.0%)	1 (9.1%)	3 (27.3%)	0 (0.0%)	4 (36.4%)
	Informational	0 (0.0%)	1 (9.1%)	2 (18.2%)	0 (0.0%)	3 (27.3%)
	Total	0 (0.0%)	4 (36.4%)	7 (63.6%)	0 (0.0%)	11 (100%)

Alert Counts by Site and Risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site: http://localhost	0 (0)	4 (4)	4 (8)	3 (11)

Alert Counts by Alert Type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	4 (36.4%)
Directory Browsing	Medium	3 (27.3%)
Hidden File Found	Medium	2 (18.2%)
Missing Anti-clickjacking Header	Medium	2 (18.2%)
Cookie without SameSite Attribute	Low	1 (9.1%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	3 (27.3%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	7 (63.6%)
X-Content-Type-Options Header Missing	Low	4 (36.4%)
Authentication Request Identified	Informational	1 (9.1%)
Session Management Response Identified	Informational	2 (18.2%)
User Agent Fuzzer	Informational	84 (763.6%)
Total		11

Alerts

Risk=Medium, Confidence=High (2)

http://localhost (2)

Content Security Policy (CSP) Header Not Set (1)

```
GET http://localhost/sitemap.xml
```

Alert tags

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06
- POLICY_QA_STD =
- POLICY_PENTEST =

Alert description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitiga
Scripting (XSS) and data injection attacks. These attacks are used for everything from da
CSP provides a set of standard HTTP headers that allow website owners to declare approv
to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images a
audio and video files.

Request

Request line and header section (230 bytes)

```
GET http://localhost/sitemap.xml HTTP/1.1
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
pragma: no-cache
cache-control: no-cache
```

Request body (0 bytes)

Response

Status line and header section (185 bytes)

```
HTTP/1.1 404 Not Found
Date: Tue, 24 Jun 2025 14:04:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Content-Length: 295
Content-Type: text/html; charset=iso-8859-1
```

Response body (295 bytes)

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at localhost
</body></html>
```

Solution

Ensure that your web server, application server, load balancer, etc. is configured to set th

Hidden File Found (1)

```
GET http://localhost/server-status
```

Alert tags

- OWASP_2021_A05
- POLICY_QA_FULL =
- POLICY_PENTEST =
- CWE-538
- WSTG-v42-CONF-05
- OWASP_2017_A06

Alert description

A sensitive file was identified as accessible or available. This may leak administrative, con

Other info

apache_server_status

Request

Request line and header section (341 bytes)

```
GET http://localhost/server-status HTTP/1.1
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
pragma: no-cache
cache-control: no-cache
referer: http://localhost/dvwa/login.php
Cookie: PHPSESSID=51k7cmcelvln9tsfk920o15a4c; security=impossible
```

Request body (0 bytes)

Response

Status line and header section (179 bytes)

```
HTTP/1.1 200 OK
Date: Tue, 24 Jun 2025 14:04:55 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Content-Length: 5267
Content-Type: text/html; charset=ISO-8859-1
```

Response body (5267 bytes)

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html><head>
<title>Apache Status</title>
</head><body>
<h1>Apache Server Status for localhost (via 127.0.0.1)</h1>

<dl><dt>Server Version: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12</dt>
<dt>Server MPM: WinNT</dt>
<dt>Apache Lounge VS17 Server built: Oct 18 2023 13:03:18
</dt></dl><hr /><dl>
<dt>Current Time: Tuesday, 24-Jun-2025 19:34:55 India Standard Time</dt>
<dt>Restart Time: Tuesday, 24-Jun-2025 17:35:42 India Standard Time</dt>
<dt>Parent Server Config. Generation: 1</dt>
<dt>Parent Server MPM Generation: 0</dt>
<dt>Server uptime:  1 hour 59 minutes 13 seconds</dt>
<dt>Server load: -1.00 -1.00 -1.00</dt>
<dt>Total accesses: 2057 - Total Traffic: 1.5 MB - Total Duration: 120535</
<dt>.288 requests/sec - 225 B/second - 785 B/request - 58.5975 ms/request</
<dt>5 requests currently being processed, 0 workers gracefully restarting, 1
</dl><pre>_____________________________________________________________________
_____________KWW_K_C</pre>
<p>Scoreboard Key:<br />
"<b><code>_</code></b>" Waiting for Connection,
"<b><code>S</code></b>" Starting up,
"<b><code>R</code></b>" Reading Request,<br />
"<b><code>W</code></b>" Sending Reply,
"<b><code>K</code></b>" Keepalive (read),
"<b><code>D</code></b>" DNS Lookup,<br />
"<b><code>C</code></b>" Closing connection,
"<b><code>L</code></b>" Logging,
"<b><code>G</code></b>" Gracefully finishing,<br />
"<b><code>I</code></b>" Idle cleanup of worker,
"<b><code>.</code></b>" Open slot with no current process<br />
</p>

<table border="0"><tr><th>Srv</th><th>PID</th><th>Acc</th><th>M</th><th>SS<

<tr><td><b>0-0</b></td><td>7600</td><td>28/69/69</td><td><b>K</b>
</td><td>0</td><td>0</td><td>2281</td><td>8.9</td><td>0.04</td><td>0.04
</td><td>127.0.0.1</td><td>http/1.1</td><td nowrap>localhost:80</td><td now

<tr><td><b>0-0</b></td><td>7600</td><td>13/322/322</td><td><b>W</b>
```

```
</td><td>0</td><td>0</td><td>6786</td><td>4.6</td><td>0.20</td><td>0.20
</td><td>127.0.0.1</td><td>http/1.1</td><td nowrap>localhost:80</td><td now

<tr><td><b>0-0</b></td><td>7600</td><td>5/136/136</td><td><b>W</b>
</td><td>0</td><td>0</td><td>25509</td><td>1.6</td><td>0.11</td><td>0.11
</td><td>127.0.0.1</td><td>http/1.1</td><td nowrap>localhost:80</td><td now

<tr><td><b>0-0</b></td><td>7600</td><td>0/209/209</td><td>_
</td><td>0</td><td>0</td><td>8225</td><td>0.0</td><td>0.16</td><td>0.16
</td><td>127.0.0.1</td><td>http/1.1</td><td nowrap>localhost:80</td><td now

<tr><td><b>0-0</b></td><td>7600</td><td>7/414/414</td><td><b>K</b>
</td><td>0</td><td>0</td><td>11503</td><td>3.8</td><td>0.35</td><td>0.35
</td><td>127.0.0.1</td><td>http/1.1</td><td nowrap>localhost:80</td><td now

<tr><td><b>0-0</b></td><td>7600</td><td>0/703/703</td><td>_
</td><td>0</td><td>15</td><td>57812</td><td>0.0</td><td>0.53</td><td>0.53
</td><td>127.0.0.1</td><td>http/1.1</td><td nowrap>localhost:80</td><td now

<tr><td><b>0-0</b></td><td>7600</td><td>1/204/204</td><td><b>C</b>
</td><td>5</td><td>0</td><td>8416</td><td>0.3</td><td>0.15</td><td>0.15
</td><td>127.0.0.1</td><td>http/1.1</td><td nowrap>localhost:80</td><td now

</table>
 <hr /> <table>
 <tr><th>Srv</th><td>Child Server number - generation</td></tr>
 <tr><th>PID</th><td>OS process ID</td></tr>
 <tr><th>Acc</th><td>Number of accesses this connection / this child / this
 <tr><th>M</th><td>Mode of operation</td></tr>
<tr><th>SS</th><td>Seconds since beginning of most recent request</td></tr>
 <tr><th>Req</th><td>Milliseconds required to process most recent request</
 <tr><th>Dur</th><td>Sum of milliseconds required to process all requests</
 <tr><th>Conn</th><td>Kilobytes transferred this connection</td></tr>
 <tr><th>Child</th><td>Megabytes transferred this child</td></tr>
 <tr><th>Slot</th><td>Total megabytes transferred this slot</td></tr>
 </table>
<hr>
<table cellspacing=0 cellpadding=0>
<tr><td bgcolor="#000000">
<b><font color="#ffffff" face="Arial,Helvetica">SSL/TLS Session Cache Statu
</td></tr>
<tr><td bgcolor="#ffffff">
cache type: <b>SHMCB</b>, shared memory: <b>512000</b> bytes, current entri
</table>
<hr />
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at localhost
</body></html>
```

Evidence `HTTP/1.1 200 OK`

Solution Consider whether or not the component is actually required in production, if it isn't then c

Risk=Medium, Confidence=Medium (2)

http://localhost (2)

Directory Browsing (1)

`GET http://localhost/dvwa/dvwa/css/`

Alert tags

- OWASP_2021_A01
- POLICY_API =
- POLICY_QA_STD =
- POLICY_QA_FULL =

- CWE-548
- POLICY_PENTEST =
- OWASP_2017_A05

Alert description

It is possible to view the directory listing. Directory listing may reveal hidden scripts, inclu

Request

Request line and header section (342 bytes)

```
GET http://localhost/dvwa/dvwa/css/ HTTP/1.1
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
pragma: no-cache
cache-control: no-cache
referer: http://localhost/dvwa/login.php
Cookie: PHPSESSID=51k7cmcelvln9tsfk920o15a4c; security=impossible
```

Request body (0 bytes)

Response

Status line and header section (173 bytes)

```
HTTP/1.1 200 OK
Date: Tue, 24 Jun 2025 14:04:50 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Content-Length: 1632
Content-Type: text/html;charset=UTF-8
```

Response body (1632 bytes)

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /dvwa/dvwa/css</title>
 </head>
 <body>
<h1>Index of /dvwa/dvwa/css</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a hre
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a hre
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a hre
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a hre
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at localhost
</body></html>
```

Attack

`http://localhost/dvwa/dvwa/css/`

Evidence

`Parent Directory`

Solution

Disable directory browsing. If this is required, make sure the listed files does not induce r

Missing Anti-clickjacking Header (1)

```
GET http://localhost/dvwa/
```

Alert tags

- OWASP_2021_A05
- POLICY_QA_STD =
- POLICY_PENTEST =
- CWE-1021

- WSTG-v42-CLNT-09
- OWASP_2017_A06

Alert description

The response does not protect against 'ClickJacking' attacks. It should include either Cont

Request

Request line and header section (224 bytes)

```
GET http://localhost/dvwa/ HTTP/1.1
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
pragma: no-cache
cache-control: no-cache
```

Request body (0 bytes)

Response

Status line and header section (299 bytes)

```
HTTP/1.1 200 OK
Date: Tue, 24 Jun 2025 14:04:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Length: 1342
Content-Type: text/html;charset=utf-8
```

Response body (1342 bytes)

```
<!DOCTYPE html>

<html lang="en-GB">

        <head>

                <meta http-equiv="Content-Type" content="text/html; charset=

                <title>Login :: Damn Vulnerable Web Application (DVWA)</titl

                <link rel="stylesheet" type="text/css" href="dvwa/css/login

        </head>

        <body>

        <div id="wrapper">

        <div id="header">

        <br />

        <p><img src="dvwa/images/login_logo.png" /></p>

        <br />

        </div> <!--<div id="header">-->

        <div id="content">

        <form action="login.php" method="post">

        <fieldset>
```

```
                                        <label for="user">Username</label> <input type="tex

                                        <label for="pass">Password</label> <input type="pas

                                        <br />

                                        <p class="submit"><input type="submit" value="Login

                        </fieldset>

                        <input type='hidden' name='user_token' value='5d71fdc5bedf5d77e866c

                        </form>

                        <br />



                        <br />
                        <br />
                        <br />
                        <br />
                        <br />
                        <br />
                        <br />
                        <br />

                        </div > <!--<div id="content">-->

                        <div id="footer">

                        <p><a href="https://github.com/digininja/DVWA/" target="_blank">Dam

                        </div> <!--<div id="footer"> -->

                        </div> <!--<div id="wrapper"> -->

                        </body>

                </html>
```

Parameter x-frame-options

Solution Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP he

If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAM
framed, you should use DENY. Alternatively consider implementing Content Security Polic

Risk=Low, Confidence=High (1)

http://localhost (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

```
GET http://localhost/sitemap.xml
```

Alert tags

- OWASP_2021_A05
- OWASP_2017_A06
- POLICY_QA_STD =
- WSTG-v42-INFO-02
- POLICY_PENTEST =
- CWE-497

Alert description	The web/application server is leaking version information via the "Server" HTTP response attackers identifying other vulnerabilities your web/application server is subject to.

Request	Request line and header section (230 bytes)
	
	`GET http://localhost/sitemap.xml HTTP/1.1`
	`host: localhost`
	`user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KI`
	`pragma: no-cache`
	`cache-control: no-cache`
	
	Request body (0 bytes)

Response	Status line and header section (185 bytes)
	
	`HTTP/1.1 404 Not Found`
	`Date: Tue, 24 Jun 2025 14:04:02 GMT`
	`Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12`
	`Content-Length: 295`
	`Content-Type: text/html; charset=iso-8859-1`
	
	Response body (295 bytes)
	
	`<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">`
	`<html><head>`
	`<title>404 Not Found</title>`
	`</head><body>`
	`<h1>Not Found</h1>`
	`<p>The requested URL was not found on this server.</p>`
	`<hr>`
	`<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at localhost`
	`</body></html>`

Evidence	`Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12`
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppr

Risk=Low, Confidence=Medium (3)

http://localhost (3)

Cookie without SameSite Attribute (1)

`GET http://localhost/dvwa/`

Alert tags	▪ OWASP_2021_A01 ▪ POLICY_QA_STD = ▪ WSTG-v42-SESS-02 ▪ POLICY_PENTEST = ▪ CWE-1275 ▪ OWASP_2017_A05 ▪ POLICY_DEV_STD =
Alert description	A cookie has been set without the SameSite attribute, which means that the cookie can b effective counter measure to cross-site request forgery, cross-site script inclusion, and tir

Request	Request line and header section (224 bytes)
	
	`GET http://localhost/dvwa/ HTTP/1.1`
	`host: localhost`
	`user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KI`

```
pragma: no-cache
cache-control: no-cache
```

Request body (0 bytes)

Response Status line and header section (660 bytes)

```
HTTP/1.1 302 Found
Date: Tue, 24 Jun 2025 14:04:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Set-Cookie: security=impossible; path=/; HttpOnly
Set-Cookie: PHPSESSID=3namh248nb1uo70mtl0tutidc7; expires=Wed, 25 Jun 2025 1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=51k7cmcelvln9tsfk920o15a4c; expires=Wed, 25 Jun 2025 1
Location: login.php
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

Response body (0 bytes)

Parameter `security`

Evidence `Set-Cookie: security`

Solution Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

```
GET http://localhost/dvwa/
```

Alert tags

- OWASP_2021_A01
- WSTG-v42-INFO-08
- POLICY_QA_STD =
- POLICY_PENTEST =
- OWASP_2017_A03
- CWE-497

Alert description The web/application server is leaking information via one or more "X-Powered-By" HTTP r
identifying other frameworks/components your web application is reliant upon and the vu

Request Request line and header section (224 bytes)

```
GET http://localhost/dvwa/ HTTP/1.1
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
pragma: no-cache
cache-control: no-cache
```

Request body (0 bytes)

Response Status line and header section (660 bytes)

```
HTTP/1.1 302 Found
Date: Tue, 24 Jun 2025 14:04:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Set-Cookie: security=impossible; path=/; HttpOnly
```

```
Set-Cookie: PHPSESSID=3namh248nb1uo70mtl0tutidc7; expires=Wed, 25 Jun 2025 1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=51k7cmcelvln9tsfk920o15a4c; expires=Wed, 25 Jun 2025 1
Location: login.php
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

Response body (0 bytes)

Evidence `X-Powered-By: PHP/8.2.12`

Solution Ensure that your web server, application server, load balancer, etc. is configured to suppr

X-Content-Type-Options Header Missing (1)

`GET http://localhost/dvwa/`

Alert tags

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06
- POLICY_QA_STD =
- POLICY_PENTEST =

Alert description The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allov response body, potentially causing the response body to be interpreted and displayed as versions of Firefox will use the declared content type (if one is set), rather than performir

Other info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often pages away from their actual content type.

At "High" threshold this scan rule will not alert on client or server error responses.

Request Request line and header section (224 bytes)

```
GET http://localhost/dvwa/ HTTP/1.1
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
pragma: no-cache
cache-control: no-cache
```

Request body (0 bytes)

Response Status line and header section (299 bytes)

```
HTTP/1.1 200 OK
Date: Tue, 24 Jun 2025 14:04:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Length: 1342
Content-Type: text/html;charset=utf-8
```

Response body (1342 bytes)

```
<!DOCTYPE html>

<html lang="en-GB">
```

```
<head>

        <meta http-equiv="Content-Type" content="text/html; charset=

        <title>Login :: Damn Vulnerable Web Application (DVWA)</tit

        <link rel="stylesheet" type="text/css" href="dvwa/css/login

</head>

<body>

<div id="wrapper">

<div id="header">

<br />

<p><img src="dvwa/images/login_logo.png" /></p>

<br />

</div> <!--<div id="header">-->

<div id="content">

<form action="login.php" method="post">

<fieldset>

                <label for="user">Username</label> <input type="text

                <label for="pass">Password</label> <input type="pass

                <br />

                <p class="submit"><input type="submit" value="Login'

</fieldset>

<input type='hidden' name='user_token' value='5d71fdc5bedf5d77e866c2

</form>

<br />



<br />
<br />
<br />
<br />
<br />
<br />
<br />
<br />

</div > <!--<div id="content">-->

<div id="footer">

<p><a href="https://github.com/digininja/DVWA/" target="_blank">Dam

</div> <!--<div id="footer"> -->
```

```
                        </div> <!--<div id="wrapper"> -->

                        </body>

                </html>
```

Parameter x-content-type-options

Solution Ensure that the application/web server sets the Content-Type header appropriately, and t

If possible, ensure that the end user uses a standards-compliant and modern web browse
application/web server to not perform MIME-sniffing.

Risk=Informational, Confidence=High (1)

http://localhost (1)

Authentication Request Identified (1)

`POST http://localhost/dvwa/login.php`

Alert tags

Alert description The given request has been identified as an authentication request. The 'Other Info' field
request is in a context which has an Authentication Method set to "Auto-Detect" then this

Other info userParam=Login

userValue=Login

passwordParam=password

referer=http://localhost/dvwa/login.php

csrfToken=user_token

Request Request line and header section (412 bytes)

```
POST http://localhost/dvwa/login.php HTTP/1.1
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
pragma: no-cache
cache-control: no-cache
content-type: application/x-www-form-urlencoded
referer: http://localhost/dvwa/login.php
content-length: 81
Cookie: PHPSESSID=51k7cmcelvln9tsfk920o15a4c; security=impossible
```

Request body (81 bytes)

```
username=ZAP&password=ZAP&Login=Login&user_token=05afc5e10e6f1d242d34cae928
```

Response Status line and header section (470 bytes)

```
HTTP/1.1 302 Found
Date: Tue, 24 Jun 2025 14:04:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=43fe12e5pt0rst71mh60usqc08; expires=Wed, 25 Jun 2025 1
Location: login.php
```

```
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

Response body (0 bytes)

Parameter Login

Evidence password

Solution This is an informational alert rather than a vulnerability and so there is nothing to fix.

Risk=Informational, Confidence=Medium (2)

http://localhost (2)

Session Management Response Identified (1)

```
GET http://localhost/dvwa/
```

Alert tags

Alert description The given response has been identified as containing a session management token. The '
Header Based Session Management Method. If the request is in a context which has a Se
the session management to use the tokens identified.

Other info cookie:security

cookie:PHPSESSID

Request Request line and header section (224 bytes)

```
GET http://localhost/dvwa/ HTTP/1.1
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
pragma: no-cache
cache-control: no-cache
```

Request body (0 bytes)

Response Status line and header section (660 bytes)

```
HTTP/1.1 302 Found
Date: Tue, 24 Jun 2025 14:04:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Set-Cookie: security=impossible; path=/; HttpOnly
Set-Cookie: PHPSESSID=3namh248nb1uo70mtl0tutidc7; expires=Wed, 25 Jun 2025
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=51k7cmcelvln9tsfk920o15a4c; expires=Wed, 25 Jun 2025
Location: login.php
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

Response body (0 bytes)

Parameter security

Evidence impossible

Solution This is an informational alert rather than a vulnerability and so there is nothing to fix.

User Agent Fuzzer (1)

```
GET http://localhost/dvwa/dvwa/css
```

Alert tags
- CUSTOM_PAYLOADS =
- POLICY_PENTEST =

Alert description Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as

Request Request line and header section (280 bytes)

```
GET http://localhost/dvwa/dvwa/css HTTP/1.1
host: localhost
user-agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
pragma: no-cache
cache-control: no-cache
referer: http://localhost/dvwa/login.php
Cookie: PHPSESSID=51k7cmcelvln9tsfk920o15a4c; security=impossible
```

Request body (0 bytes)

Response Status line and header section (173 bytes)

```
HTTP/1.1 200 OK
Date: Tue, 24 Jun 2025 14:04:57 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Content-Length: 1632
Content-Type: text/html;charset=UTF-8
```

Response body (1632 bytes)

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /dvwa/dvwa/css</title>
 </head>
 <body>
<h1>Index of /dvwa/dvwa/css</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a hre
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a hre
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a hre
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a hre
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at localhost
</body></html>
```

Parameter Header User-Agent

Attack Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

Appendix

Alert Types

This section contains additional information on the types of alerts in the report.

Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy ▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.l ▪ https://www.w3.org/TR/CSP/ ▪ https://w3c.github.io/webappsec-csp/ ▪ https://web.dev/articles/csp ▪ https://caniuse.com/#feat=contentsecuritypolicy ▪ https://content-security-policy.com/

Directory Browsing

Source	raised by an active scanner (Directory Browsing)
CWE ID	548
WASC ID	48
Reference	▪ https://httpd.apache.org/docs/mod/core.html#options

Hidden File Found

Source	raised by an active scanner (Hidden File Finder)
CWE ID	538
WASC ID	13
Reference	▪ https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html ▪ https://httpd.apache.org/docs/current/mod/mod_status.html

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Cookie without SameSite Attribute

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
CWE ID	497
WASC ID	13
Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework ▪ https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	497
WASC ID	13
Reference	▪ https://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) ▪ https://www.troyhunt.com/shhh-dont-let-your-response-headers/

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	▪ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) ▪ https://owasp.org/www-community/Security_Headers

Authentication Request Identified

Source	raised by a passive scanner (Authentication Request Identified)
Reference	

- https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

Session Management Response Identified

Source	raised by a passive scanner (Session Management Response Identified)
Reference	- https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id

User Agent Fuzzer

Source	raised by an active scanner (User Agent Fuzzer)
Reference	- https://owasp.org/wstg