# ZAP Scanning Report

Generated with ZAP on Wed 21 Feb 2024, at 13:49:35

ZAP Version: 2.14.0

## Contents



## About this report

### Report description

DVWA Impossible scan

### 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 (16.7%) | 2 (16.7%) | 0 (0.0%) | 4 (33.3%) |
| | Low | 0 (0.0%) | 1 (8.3%) | 3 (25.0%) | 0 (0.0%) | 4 (33.3%) |
| | Informational | 0 (0.0%) | 1 (8.3%) | 2 (16.7%) | 1 (8.3%) | 4 (33.3%) |
| | Total | 0 (0.0%) | 4 (33.3%) | 7 (58.3%) | 1 (8.3%) | 12 (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) | 4 (12) |

## 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 (33.3%) |
| Directory Browsing | Medium | 3 (25.0%) |
| Hidden File Found | Medium | 2 (16.7%) |
| Missing Anti-clickjacking Header | Medium | 2 (16.7%) |
| Cookie without SameSite Attribute | Low | 1 (8.3%) |
| Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) | Low | 3 (25.0%) |
| Server Leaks Version Information via "Server" HTTP Response Header Field | Low | 7 (58.3%) |
| X-Content-Type-Options Header Missing | Low | 4 (33.3%) |
| Authentication Request Identified | Informational | 1 (8.3%) |
| Loosely Scoped Cookie | Informational | 2 (16.7%) |
| Total | | 12 |

| Alert type | Risk | Count |
|---|---|---|
| Session Management Response Identified | Informational | 4 (33.3%) |
| User Agent Fuzzer | Informational | 84 (700.0%) |
| Total | | 12 |

# Alerts

**Risk=Medium, Confidence=High (2)**

**http://localhost (2)**

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

▼ GET http://localhost/sitemap.xml

**Alert tags**

- OWASP_2021_A05
- OWASP_2017_A06

**Alert description**

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. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, 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 (KHTML, like Gecko) Chrome/116.0.0.0
Safari/537.36
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: Wed, 21 Feb 2024 19:44:34 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 Port 80</address>
</body></html>
```

**Solution** Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

## Hidden File Found (1)

▼ GET http://localhost/server-status

**Alert tags**
- OWASP_2021_A05
- WSTG-v42-CONF-05
- OWASP_2017_A06

**Alert description** A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

**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 (KHTML, like Gecko) Chrome/116.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: http://localhost/DVWA/login.php
Cookie: PHPSESSID=ah8itig3mgi0hophqqqbenrc8t;
security=impossible
```

▼ Request body (0 bytes)

**Response** ▼ Status line and header section (179 bytes)

```
HTTP/1.1 200 OK
Date: Wed, 21 Feb 2024 19:46:20 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Content-Length: 5272
Content-Type: text/html; charset=ISO-8859-1
```

▼ Response body (5272 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: Wednesday, 21-Feb-2024 13:46:20 Central
Standard Time</dt>
<dt>Restart Time: Wednesday, 21-Feb-2024 13:42:00 Central
Standard Time</dt>
<dt>Parent Server Config. Generation: 1</dt>
<dt>Parent Server MPM Generation: 0</dt>
<dt>Server uptime:  4 minutes 20 seconds</dt>
<dt>Server load: -1.00 -1.00 -1.00</dt>
<dt>Total accesses: 2116 - Total Traffic: 1.8 MB - Total
Duration: 113256</dt>
<dt>8.14 requests/sec - 6.9 kB/second - 869 B/request -
53.5236 ms/request</dt>
<dt>4 requests currently being processed, 0 workers
gracefully restarting, 146 idle workers</dt>
</dl>
<pre>_____________________________________________________
__________
_____________________________________________W_______
_____
___WK_____________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</th><th>Req</th><th>Dur</th><th>Conn</th>
<th>Child</th><th>Slot</th><th>Client</th><th>Protocol</th>
<th>VHost</th><th>Request</th></tr>

<tr><td><b>0-0</b></td><td>12168</td><td>0/336/336</td>
<td>_
</td><td>5</td><td>30</td><td>18015</td><td>0.0</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 nowrap>POST /DVWA/login.php
HTTP/1.1</td></tr>

<tr><td><b>0-0</b></td><td>12168</td><td>10/340/340</td>
```

<td>W
</td><td>0</td><td>0</td><td>18722</td><td>3.0</td>
<td>0.32</td><td>0.32
</td><td>127.0.0.1</td><td>http/1.1</td><td
nowrap>localhost:80</td><td nowrap>POST /DVWA/login.php
HTTP/1.1</td></tr>

<tr><td>0-0</td><td>12168</td><td>16/322/322</td>
<td>W
</td><td>0</td><td>0</td><td>16030</td><td>5.9</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 nowrap>GET /server-status
HTTP/1.1</td></tr>

<tr><td>0-0</td><td>12168</td><td>5/324/324</td><td>
K
</td><td>0</td><td>0</td><td>16463</td><td>1.5</td>
<td>0.26</td><td>0.26
</td><td>127.0.0.1</td><td>http/1.1</td><td
nowrap>localhost:80</td><td nowrap>GET /DVWA/dvwa/images
HTTP/1.1</td></tr>

<tr><td>0-0</td><td>12168</td><td>0/443/443</td>
<td>_
</td><td>0</td><td>1</td><td>23415</td><td>0.0</td>
<td>0.52</td><td>0.52
</td><td>127.0.0.1</td><td>http/1.1</td><td
nowrap>localhost:80</td><td nowrap>GET /lfm.php
HTTP/1.1</td></tr>

<tr><td>0-0</td><td>12168</td><td>3/245/245</td><td>
C
</td><td>5</td><td>0</td><td>14355</td><td>1.6</td>
<td>0.17</td><td>0.17
</td><td>127.0.0.1</td><td>http/1.1</td><td
nowrap>localhost:80</td><td nowrap>GET
/DVWA/dvwa/images/login_logo.png/ HTTP/1.1</td></tr>

<tr><td>0-0</td><td>12168</td><td>0/106/106</td>
<td>_
</td><td>2</td><td>18</td><td>6253</td><td>0.0</td>
<td>0.07</td><td>0.07
</td><td>127.0.0.1</td><td>http/1.1</td><td
nowrap>localhost:80</td><td nowrap>POST /DVWA/login.php
HTTP/1.1</td></tr>

</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 slot</td></tr>
 <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</td></tr>
 <tr><th>Dur</th><td>Sum of milliseconds required to
process all requests</td></tr>

```
 <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 Status:</font></b>
</td></tr>
<tr><td bgcolor="#ffffff">
cache type: <b>SHMCB</b>, shared memory: <b>512000</b>
bytes, current entries: <b>0</b><br>subcaches: <b>32</b>,
indexes per subcache: <b>88</b><br>index usage: <b>0%</b>,
cache usage: <b>0%</b><br>total entries stored since
starting: <b>0</b><br>total entries replaced since
starting: <b>0</b><br>total entries expired since
starting: <b>0</b><br>total (pre-expiry) entries scrolled
out of the cache: <b>0</b><br>total retrieves since
starting: <b>0</b> hit, <b>0</b> miss<br>total removes
since starting: <b>0</b> hit, <b>0</b> miss<br></td></tr>
</table>
<hr />
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Server at localhost Port 80</address>
</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 disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.

## Risk=Medium, Confidence=Medium (2)

### http://localhost (2)

#### Directory Browsing (1)

▼ GET http://localhost/DVWA/dvwa/images/

**Alert tags**
- OWASP_2021_A01
- OWASP_2017_A05

**Alert description** It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.

**Request** ▼ Request line and header section (345 bytes)

```
GET http://localhost/DVWA/dvwa/images/ HTTP/1.1
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0
```

```
Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: http://localhost/DVWA/login.php
Cookie: PHPSESSID=ah8itig3mgi0hophqqqbenrc8t;
security=impossible
```

▼ Request body (0 bytes)

**Response**

▼ Status line and header section (173 bytes)

```
HTTP/1.1 200 OK
Date: Wed, 21 Feb 2024 19:46:15 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Content-Length: 2079
Content-Type: text/html;charset=UTF-8
```

▼ Response body (2079 bytes)

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /DVWA/dvwa/images</title>
 </head>
 <body>
<h1>Index of /DVWA/dvwa/images</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="
[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?
C=S;O=A">Size</a></th><th><a href="?
C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="
[PARENTDIR]"></td><td><a href="/DVWA/dvwa/">Parent
Directory</a>       </td><td> </td><td
align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="
[IMG]"></td><td><a href="dollar.png">dollar.png</a>
      </td><td align="right">2024-01-29 04:42  </td><td
align="right">299 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="
[IMG]"></td><td><a href="lock.png">lock.png</a>
    </td><td align="right">2024-01-29 04:42  </td><td
align="right">761 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="
[IMG]"></td><td><a
href="login_logo.png">login_logo.png</a>         </td><td
align="right">2024-01-29 04:42  </td><td
align="right">8.9K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="
[IMG]"></td><td><a href="logo.png">logo.png</a>
    </td><td align="right">2024-01-29 04:42  </td><td
align="right">4.9K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="
[IMG]"></td><td><a href="spanner.png">spanner.png</a>
       </td><td align="right">2024-01-29 04:42  </td><td
align="right">464 </td><td> </td></tr>
```

<tr><td valign="top"><img src="/icons/image2.gif" alt="
[IMG]"></td><td><a href="warning.png">warning.png</a>
</td><td align="right">2024-01-29 04:42 </td><td
align="right">423 </td><td> </td></tr>
<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 Port 80</address>
</body></html>

**Attack** http://localhost/DVWA/dvwa/images/

**Evidence** Parent Directory

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

## Missing Anti-clickjacking Header (1)

▼ GET http://localhost/DVWA/

**Alert tags**
- OWASP_2021_A05
- WSTG-v42-CLNT-09
- OWASP_2017_A06

**Alert description** The response does not include either Content-Security-Policy with 'frame-ancestors' directiv

**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 (KHTML, lik
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: Wed, 21 Feb 2024 19:44:34 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=UTF-8" /
        <title>Login :: Damn Vulnerable Web Application (DVWA)</title>
        <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />
</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" class=

                <label for="pass">Password</label> <input type="password" cl
                <br />
                <p class="submit"><input type="submit" value="Login" name="L
</fieldset>
<input type='hidden' name='user_token' value='1ac2f70fa177785e3d585277b3bdcf
</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">Damn Vulnera

                        </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 head site/app.

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

### Risk=Low, Confidence=High (1)

#### http://localhost (1)

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

▼ GET http://localhost/DVWA/dvwa/css/login.css

**Alert tags**
- OWASP_2021_A05
- OWASP_2017_A06
- WSTG-v42-INFO-02

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

**Request** ▼ Request line and header section (351 bytes)

```
GET http://localhost/DVWA/dvwa/css/login.css HTTP/1.1
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: http://localhost/DVWA/login.php
Cookie: PHPSESSID=ah8itig3mgi0hophqqqbenrc8t;
security=impossible
```

▼ Request body (0 bytes)

**Response** ▼ Status line and header section (252 bytes)

```
HTTP/1.1 200 OK
Date: Wed, 21 Feb 2024 19:44:34 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Last-Modified: Mon, 29 Jan 2024 10:42:04 GMT
```

```
ETag: "34a-610134be53700"
Accept-Ranges: bytes
Content-Length: 842
Content-Type: text/css
```

▼ Response body (842 bytes)

```
body {
        background: #fefffe;
        font: 12px/15px Arial, Helvetica, sans-serif;
        line-height: 20px;
        color: #6b6b6b;
}

#wrapper {
        text-align: center;
        margin: 0 auto;
}

#content {
        display: inline-block;
        padding: 20px;
        width: auto;
}

#footer {
        position: absolute;
        width: 100%;
        height: 50px;
        bottom: 0px;
        left: 0px;
}

label {
        float: left;
        text-align: right;
        margin-right: 0.5em;
        display: block;
        overflow: hidden;
        padding-right: 50px;
        font-weight: bold;
}

.loginInput {
        float: left;
        color: #6B6B6B;
        width: 320px;
        background-color: #F4F4F4;
        border: 1px;
        border-style: solid;
        border-color: #c4c4c4;
        padding: 6px;
        margin-bottom: 12px;
}

fieldset {
        width: 350px;
        padding: 10px 20px 10px 20px;
        overflow: hidden;
        border-style: none;
```

```
}

p {
        font-size: 10px;
}
```

**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 suppress the "Server" header or provide generic details.

## Risk=Low, Confidence=Medium (3)

### http://localhost (3)

### Cookie without SameSite Attribute (1)

▼ GET http://localhost/DVWA/

**Alert tags**

- OWASP_2021_A01
- WSTG-v42-SESS-02
- OWASP_2017_A05

**Alert description** A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

**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 (KHTML, like Gecko) Chrome/116.0.0.0
Safari/537.36
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: Wed, 21 Feb 2024 19:44:34 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=1etlbkcbqcrkg0uk9sik1dquis;
expires=Thu, 22 Feb 2024 19:44:34 GMT; Max-Age=86400;
path=/; HttpOnly; SameSite=Strict
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
```

```
Set-Cookie: PHPSESSID=ah8itig3mgi0hophqqqbenrc8t;
expires=Thu, 22 Feb 2024 19:44:34 GMT; Max-Age=86400;
path=/; HttpOnly; SameSite=Strict
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
- OWASP_2017_A03

**Alert description** The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

**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 (KHTML, like Gecko) Chrome/116.0.0.0
Safari/537.36
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: Wed, 21 Feb 2024 19:44:34 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=1etlbkcbqcrkg0uk9sik1dquis;
expires=Thu, 22 Feb 2024 19:44:34 GMT; Max-Age=86400;
path=/; HttpOnly; SameSite=Strict
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=ah8itig3mgi0hophqqqbenrc8t;
```

```
expires=Thu, 22 Feb 2024 19:44:34 GMT; Max-Age=86400;
path=/; HttpOnly; SameSite=Strict
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 suppress "X-Powered-By" headers.

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

▼ `GET http://localhost/DVWA/dvwa/css/login.css`

**Alert tags**
- OWASP_2021_A05
- OWASP_2017_A06

**Alert description** The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

**Other info** This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing 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 (351 bytes)

```
GET http://localhost/DVWA/dvwa/css/login.css HTTP/1.1
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: http://localhost/DVWA/login.php
Cookie: PHPSESSID=ah8itig3mgi0hophqqqbenrc8t;
security=impossible
```

▼ Request body (0 bytes)

**Response** ▼ Status line and header section (252 bytes)

```
HTTP/1.1 200 OK
Date: Wed, 21 Feb 2024 19:44:34 GMT
```

```
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Last-Modified: Mon, 29 Jan 2024 10:42:04 GMT
ETag: "34a-610134be53700"
Accept-Ranges: bytes
Content-Length: 842
Content-Type: text/css
```

▼ Response body (842 bytes)

```
body {
        background: #fefffe;
        font: 12px/15px Arial, Helvetica, sans-serif;
        line-height: 20px;
        color: #6b6b6b;
}

#wrapper {
        text-align: center;
        margin: 0 auto;
}

#content {
        display: inline-block;
        padding: 20px;
        width: auto;
}

#footer {
        position: absolute;
        width: 100%;
        height: 50px;
        bottom: 0px;
        left: 0px;
}

label {
        float: left;
        text-align: right;
        margin-right: 0.5em;
        display: block;
        overflow: hidden;
        padding-right: 50px;
        font-weight: bold;
}

.loginInput {
        float: left;
        color: #6B6B6B;
        width: 320px;
        background-color: #F4F4F4;
        border: 1px;
        border-style: solid;
        border-color: #c4c4c4;
        padding: 6px;
        margin-bottom: 12px;
}

fieldset {
        width: 350px;
        padding: 10px 20px 10px 20px;
```

```
        overflow: hidden;
        border-style: none;
}

p {
        font-size: 10px;
}
```

**Parameter** x-content-type-options

**Solution** Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web 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 contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.

**Other info** userParam=Login

userValue=Login

passwordParam=password

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

**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 (KHTML, like Gecko) Chrome/116.0.0.0
Safari/537.36
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=ah8itig3mgi0hophqqqbenrc8t;
```

security=impossible

▼ Request body (81 bytes)

username=ZAP&password=ZAP&Login=Login&user_token=c73110c57
53aea12eda6108cd806c71a

**Response**

▼ Status line and header section (470 bytes)

```
HTTP/1.1 302 Found
Date: Wed, 21 Feb 2024 19:44:34 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=jhc1beuo31t9cr3v9pi3vnugr5;
expires=Thu, 22 Feb 2024 19:44:34 GMT; Max-Age=86400;
path=/; HttpOnly; SameSite=Strict
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 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change 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 (KHTML, like Gecko) Chrome/116.0.0.0
Safari/537.36
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: Wed, 21 Feb 2024 19:44:34 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=1etlbkcbqcrkg0uk9sik1dquis;
expires=Thu, 22 Feb 2024 19:44:34 GMT; Max-Age=86400;
path=/; HttpOnly; SameSite=Strict
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=ah8itig3mgi0hophqqqbenrc8t;
expires=Thu, 22 Feb 2024 19:44:34 GMT; Max-Age=86400;
path=/; HttpOnly; SameSite=Strict
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

**Alert tags**

**Alert description** Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a hashcode of the response body with the original response.

**Request**

▼ Request line and header section (162 bytes)

```
GET http://localhost/DVWA 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

▼ Request body (0 bytes)

**Response**

▼ Status line and header section (628 bytes)

```
HTTP/1.1 200 OK
Date: Wed, 21 Feb 2024 19:46:21 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=gmobegsju9v4b8k9q0lsg1ca8p; expires=Thu, 22 Feb 2024 19:46:21
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=09cie8jjioate8p9vkon5iidfa; expires=Thu, 22 Feb 2024 19:46:21
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=UTF-8" /

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

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

        </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" class=
```

```
                                        <label for="pass">Password</label> <input type="password" cl

                                        <br />

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

                                </fieldset>

                                <input type='hidden' name='user_token' value='4ac5573408a935b2eba437674966b4

                                </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">Damn Vulnera

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

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

                                </body>

                        </html>
```

**Parameter** Header User-Agent

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

## Risk=Informational, Confidence=Low (1)

### http://localhost (1)

#### Loosely Scoped Cookie (1)

▼ GET http://localhost/DVWA/

**Alert tags**

- WSTG-v42-SESS-02
- OWASP_2021_A08
- OWASP_2017_A06

**Alert description** Cookies can be scoped by domain or path. This check is only concerned with domain scope.The domain scope applied to a cookie determines which domains can access it. For example, a

cookie can be scoped strictly to a subdomain e.g. www.nottrusted.com, or loosely scoped to a parent domain e.g. nottrusted.com. In the latter case, any subdomain of nottrusted.com can access the cookie. Loosely scoped cookies are common in mega-applications like google.com and live.com. Cookies set from a subdomain like app.foo.bar are transmitted only to that domain by the browser. However, cookies scoped to a parent-level domain may be transmitted to the parent, or any subdomain of the parent.

**Other info**

The origin domain used for comparison was:

localhost

security=impossible

PHPSESSID=1etlbkcbqcrkg0uk9sik1dquis

PHPSESSID=ah8itig3mgi0hophqqqbenrc8t

**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 (KHTML, like Gecko) Chrome/116.0.0.0
Safari/537.36
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: Wed, 21 Feb 2024 19:44:34 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=1etlbkcbqcrkg0uk9sik1dquis;
expires=Thu, 22 Feb 2024 19:44:34 GMT; Max-Age=86400;
path=/; HttpOnly; SameSite=Strict
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=ah8itig3mgi0hophqqqbenrc8t;
expires=Thu, 22 Feb 2024 19:44:34 GMT; Max-Age=86400;
path=/; HttpOnly; SameSite=Strict
Location: login.php
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

▼ Response body (0 bytes)

**Solution**

Always scope cookies to a FQDN (Fully Qualified Domain Name).

# 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<br>• https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html<br>• https://www.w3.org/TR/CSP/<br>• https://w3c.github.io/webappsec-csp/<br>• https://web.dev/articles/csp<br>• https://caniuse.com/#feat=contentsecuritypolicy<br>• 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<br>• 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** | 200 |
| **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<br>▪ 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** | 200 |
| **WASC ID** | 13 |
| **Reference** | ▪ https://httpd.apache.org/docs/current/mod/core.html#servertokens<br>▪ https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)<br>▪ 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)<br>▪ 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/ |

### Loosely Scoped Cookie

| | |
|---|---|
| **Source** | raised by a passive scanner (Loosely Scoped Cookie) |
| **CWE ID** | 565 |
| **WASC ID** | 15 |
| **Reference** | ▪ https://tools.ietf.org/html/rfc6265#section-4.1<br>▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html<br>▪ https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies |

### 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 |