Vooki Pro Version

Dynamic Application Security Testing Report

Target: http://localhost/dvwa

VOOKI
INFOSEC

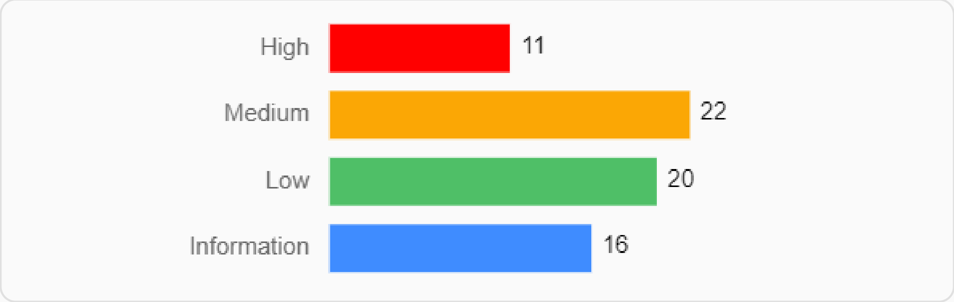
Scan information

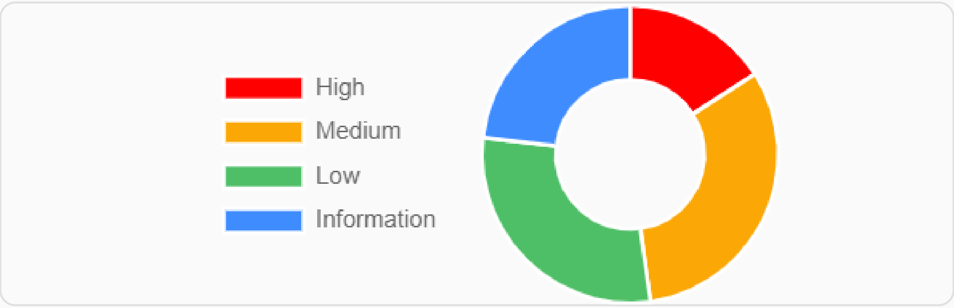
Target	http://localhost/dvwa	Scan Type	Full Scan
Scan Status	Completed	Scan Duration	0:1:26
Start Time	27-Sept-2023 11:04:27 AM	End Time	27-Sept-2023 11:05:54 AM
Requests	829	Report Type	Standard

Identified Vulnerabilities

IDENTIFIED	HIGH	MEDIUM	LOW	INFORMATION
69	11	22	20	16

Vulnerability Analysis





Vulnerability Findings

No	VULNERABILITY	RISK	SEVERITY	OCCURRENCES
1	Sql injection - MySQL	High	High	2
2	Blind Sql injection - MySQL	High	High	2
3	Weak password detected	High	High	1
4	Insecure communication detected	High	High	4
5	Directory listing	High	High	2
6	Cross site scripting - reflected	Medium	Medium	5
7	Verb tampering	Medium	Medium	2
8	Technical information exposure on the webpage	Medium	Medium	2
9	Sensitive information disclosure in response headers - x-powered-by	Medium	Medium	6
10	Sensitive information disclosure in response headers - server	Medium	Medium	6
11	Error Messages Detected	Medium	Medium	1
12	Possible Cross-Site Request Forgery Attack Detected	Low	Low	1
13	Missing security headers - X-Frame-Options	Low	Low	5
14	Missing security headers - X-Content-Type-Options	Low	Low	5
15	Missing Content Security Policy in response header	Low	Low	6
16	HTTP trace support detected	Low	Low	1
17	Autocomplete on sensitive fields	Low	Low	1
18	Autocomplete on password fields	Low	Low	1
19	Missing security headers - X-XSS-Protection	Information	Information	4
20	Missing header - Permissions-Policy	Information	Information	5
21	Missing header - Expect-CT	Information	Information	5
22	Direct dynamic code execution - eval injection	Information	Information	2

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 1 Sql injection - MySQL

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
High	High	8.8	2

Description

Vooki identified a SQL injection vulnerability in the following URL http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit. The payload ' was submitted using HTTP GET method. The HTTP response of http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit appears to contain the output from the injected payload, indicating that the payload was executed successfully on the server.Check the highlighted payload, method and response of modified request in the request/response section.

A SQL injection attack consists of the insertion or injection of a SQL query via the client's input data to the application. SQL injection attack is a type of attack wherein malicious SQL commands are injected into data-plane input to affect the execution of predefined SQL commands.
A successful SQL injection attack can

- Read sensitive data from the database.
- Modify the database data (Insert/Update/Delete).
- Execute administration operations on the database (such as shutdown the DBMS).
- Recover the content of a given file present on the DBMS file system.
- In some cases, issue malicious commands to the operating system.

Remediation

SQL Injection flaws are introduced when software developers create dynamic database queries that includes user-supplied input. Techniques for preventing SQL Injection vulnerabilities are:

- Use of prepared statements (with Parameterized Queries)
- Use of stored procedures (only in java)
- Whitelist input validation.
- Escape all user-supplied inputs.

Classification:	OWASP 2021: A3, OWASP 2017: A1, OWASP API 2019: API8, PCI-DSS: 3.2.1-6.5.1, CWE: 89
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Url: http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit
Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/vulnerabilities/sqli/ upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:34:49 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache content-length: 162 keep-alive: timeout=5, max=100 connection: Keep-Alive content-type: text/html; charset=UTF-8 status code: 200 <pre>You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''''' at line 1</pre>

Url: http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit='
Occurrences in this Url: 1

Request

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/vulnerabilities/sqli/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572
```

Response

```
date: Wed, 27 Sep 2023 05:34:49 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate
pragma: no-cache
content-length: 162
keep-alive: timeout=5, max=2
connection: Keep-Alive
content-type: text/html; charset=UTF-8
status code: 200

<pre>You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '''' at line 1</pre>
```

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 2 Blind Sql injection - MySQL

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
High	High	8.8	2

Description

Vooki identified a blind SQL injection vulnerability in the following URL http://localhost/dvwa/vulnerabilities/sqli/?id=1%27%20AND%20SLEEP(25)%23&Submit=Submit. The payload 1%27%20AND%20SLEEP(25)%23 was submitted using HTTP GET method. The HTTP response of http://localhost/dvwa/vulnerabilities/sqli/?id=1%27%20AND%20SLEEP(25)%23&Submit=Submit arrived after 25 seconds which indicates that the payload was executed successfully on the server. Check the highlighted payload, method and HTTP response of modified request in the request/response section.

Remediation

SQL Injection flaws are introduced when software developers create dynamic database queries that includes user-supplied input. Techniques for preventing SQL Injection vulnerabilities are:

- Use of prepared statements (with Parameterized Queries)
- Use of stored procedures (only in java)
- Whitelist input validation.
- Escape all user-supplied inputs.

Classification:	OWASP 2021: A1, OWASP 2017: A3, OWASP API 2019: API8, PCI-DSS: 3.2.1-6.5.1, CWE: 89
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Url:	http://localhost/dvwa/vulnerabilities/sqli/?id=1' AND SLEEP(25)%23&Submit=Submit
Occurrences in this Url:	1

Request

Method: GET

user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0

accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

accept-language: en-US,en;q=0.5

referer: http://localhost/dvwa/vulnerabilities/sqli/

upgrade-insecure-requests: 1

sec-fetch-dest: document

sec-fetch-site: same-origin

sec-fetch-user: ?1

connection: keep-alive

cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572

Response

date: Wed, 27 Sep 2023 05:35:01 GMT

server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30

x-powered-by: PHP/7.4.30

expires: Tue, 23 Jun 2009 12:00:00 GMT

cache-control: no-cache, must-revalidate

pragma: no-cache

content-length: 4207

keep-alive: timeout=5, max=59

connection: Keep-Alive

content-type: text/html;charset=utf-8

status code: 200

Url:	http://localhost/dvwa/vulnerabilities/sqli_blind/?id=1' AND SLEEP(25)%23&Submit=Submit
Occurrences in this Url:	1

Request

Method: GET

user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0

accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

accept-language: en-US,en;q=0.5

referer: http://localhost/dvwa/vulnerabilities/sqli_blind/

Response

date: Wed, 27 Sep 2023 05:35:27 GMT

server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30

x-powered-by: PHP/7.4.30

expires: Tue, 23 Jun 2009 12:00:00 GMT

cache-control: no-cache, must-revalidate

pragma: no-cache

content-length: 4317

keep-alive: timeout=5, max=9

```
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low;
PHPSESSID=592pnf1jafdckauam7unlp9572
```

```
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 404
```

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 3 Weak password detected

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
High	High	7.5	1

Description

Vooki has detected a weak password in the URL http://localhost/dvwa/login.php. A weak password is one that is short, common, a system default, or anything that might be quickly guessed by performing a brute force attack utilizing a subset of all possible passwords, such as dictionary terms, proper names, words based on the user name, or popular variations on these themes.

Remediation

Implement a strong password policy that includes the following:

- One or more uppercase characters
- One or more numerical digits
- One or more special characters
- Minimum length of 8 characters
- Disallow any part of the username
- Disallow dictionary words
- Disallow any character more than three times in succession
- Disallow previously used passwords

Classification:	OWASP 2021: A7, OWASP 2017: A2, OWASP API 2019: API2, PCI-DSS: 3.2.1-6.5.10, CWE: 521
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Url:	http://localhost/dvwa/login.php
Occurrences in this Url:	1

Request

Method: POST

host: localhost

user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0

accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

accept-language: en-US,en;q=0.5

accept-encoding: gzip, deflate

content-type: application/x-www-form-urlencoded

content-length: 88

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

origin: http://localhost

upgrade-insecure-requests: 1

sec-fetch-dest: document

sec-fetch-mode: navigate

sec-fetch-site: same-origin

sec-fetch-user: ?1

connection: keep-alive

cookie: security=impossible; PHPSESSID=592pnf1jafdckauam7unlp9572

Login=Login&password=password&user_token=c3f83edcde56e1e228b7ddfca91d85dd&username=admin

Response

date: Wed, 27 Sep 2023 05:30:13 GMT

server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30

x-powered-by: PHP/7.4.30

expires: Thu, 19 Nov 1981 08:52:00 GMT

cache-control: no-store, no-cache, must-revalidate

pragma: no-cache

location: index.php

content-length: 0

keep-alive: timeout=5, max=100

connection: Keep-Alive

content-type: text/html; charset=UTF-8

status code: 302

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 4 Insecure communication detected

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
High	High	7.5	4

Description

Vooki has detected an insecure communication vulnerability in the URL http://localhost/dvwa/login.php.When a client and server interact through an insecure (unencrypted) link, insecure communications occur. The developer cannot ensure the confidentiality and integrity of the data unless the channel is encrypted.

Remediation

Ensure that every client-server connection is secured using an SSL certificate that is authentic and has the appropriate encryption.

Classification:	OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5.4, CWE: 319
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Url:	http://localhost/dvwa/login.php
Occurrences in this Url:	1

Request

Method: GET
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate
connection: keep-alive
cookie: security=impossible; PHPSESSID=1klskcb5cr1o6aakt71rij3nbu

Response

date: Wed, 27 Sep 2023 04:28:03 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 1415
keep-alive: timeout=5, max=98
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

Url:	http://localhost/dvwa/vulnerabilities/sqli
Occurrences in this Url:	1

Request

Method: GET
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate
referer: http://localhost/dvwa/security.php
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-mode: navigate
sec-fetch-site: same-origin
sec-fetch-user: ?1

Response

date: Wed, 27 Sep 2023 05:30:46 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 4207
keep-alive: timeout=5, max=100
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

```
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572
```

Url: http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit

Occurrences in this Url: 1

Request

```
Method: GET
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate
referer: http://localhost/dvwa/vulnerabilities/sqli/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-mode: navigate
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572
```

Response

```
date: Wed, 27 Sep 2023 05:31:50 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate
pragma: no-cache
content-length: 162
keep-alive: timeout=5, max=100
connection: Keep-Alive
content-type: text/html; charset=UTF-8
status code: 200
```

Url: http://localhost/dvwa/vulnerabilities/xss_r/?name=123

Occurrences in this Url: 1

Request

```
Method: GET
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate
referer: http://localhost/dvwa/vulnerabilities/xss_r/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-mode: navigate
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572
```

Response

```
date: Wed, 27 Sep 2023 05:32:45 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
x-xss-protection: 0
content-length: 4214
keep-alive: timeout=5, max=100
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200
```

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 5 Directory listing

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
High	High	7.5	2

Description

Vooki has detected a directory listing issue in the application URL http://localhost/dvwa/dvwa/images/. Directory listing is a web server feature that displays the directory contents when there is no index file in a specific website directory. A directory listing vulnerability occurs when a webserver lists the contents of its directories, allowing an attacker to simply browse all of the files included within the affected folders.
Reference:
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

Remediation

It is advised to disable directory listing on the web server.

Classification:	OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5.8, CWE: 548
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Url: http://localhost/dvwa/dvwa/images/
Occurrences in this Url: 1

Request

Method: GET

Response

```
date: Wed, 27 Sep 2023 05:34:41 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
content-length: 2298
keep-alive: timeout=5, max=73
connection: Keep-Alive
content-type: text/html;charset=UTF-8
status code: 200

<!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=
```

Url: http://localhost/dvwa/dvwa/
Occurrences in this Url: 1

Request

Method: GET

Response

```
date: Wed, 27 Sep 2023 05:34:41 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
content-length: 1616
keep-alive: timeout=5, max=71
```

```
connection: Keep-Alive
content-type: text/html;charset=UTF-8
status code: 200

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//E
N">
<html>
 <head>
  <title>Index of /dvwa/dvwa</title>
 </head>
 <body>
<h1>Index of /dvwa/dvwa</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[I
CO]"></th><th><a href="?C=N;O=D">Name</a></th><th
><a href="?C=M;O=A">Last modified</a></th><th><a hre
f="?C=S;O=A">
```

Payloads and Evidence are highlighted in the red color

Findings: 6 Cross site scripting - reflected

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Medium	Medium	6.5	5

Description

Vooki identified a Cross-Site Scripting – Reflected vulnerability in the URL http://localhost/dvwa/vulnerabilities/sqli. GET method was used to submit the payload . Cross-Site Scripting (XSS) attacks occur when malicious javascripts are injected into a website's input fields and the website processes them without input encoding, input validation, or XSS filters. XSS attacks occur when an attacker utilizes a web application to transmit malicious code to a separate end-user, typically in the form of a browser side script.

Remediation

- Before running any user-provided inputs, clean them all up. Never allow your application code to output the outcome of received input data without first validating it.
- Before adding untrusted data to HTML URL parameter values, URL encoding is required.
- Before adding untrusted data to JavaScript data values, JavaScript must be encoded.
- As extra layers of security defense, provide CSP and XSS protection headers on the client and server sides.

Classification:	OWASP 2021: A1, OWASP 2017: A3, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5.7, CWE: 79
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

Url:	http://localhost/dvwa/vulnerabilities/sqli
Occurrences in this Url:	1

Request

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/security.php
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=<script>alert(123)</script>; PHPSESSID=592pnf1jafdckauam7unlp9572;
```

Response

```
date: Wed, 27 Sep 2023 05:34:46 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
set-cookie: PHPSESSID=592pnf1jafdckauam7unlp9572; path=/; HttpOnly,security=impossible; HttpOnly
content-length: 4347
keep-alive: timeout=5, max=10
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

="clear">
        </div>

        <div id="system_info">
            <input type="button" value="View Help" class="popup_button" id='help_button' data-help-url='../../vulnerabilities/view_help.php?id=sqli&security=<script>alert(123)</script>' )"> <input type="button" value="View Source" class="popup_button" id='source_button' data-source-url='../../vulnerabilities/view_source.php?id=sqli&security=

' )"> <input type="button" value="View Source" class="popup_button" id='source_button' data-source-url='../../vuln
```

```
erabilities/view_source.php?id=sqli&security=<script>alert(123)</script>' )"> <div align="left"><em>Username:</em> admin<br /><em>Security Level:</em> impossible<br /><em>PHPIDS:</em> disabled</div>
		</div>

		<div id="footer">

			<p>Damn Vulnerable Web Applicat
```

Url: http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit

Occurrences in this Url: 1

Request	Response

Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/vulnerabilities/sqli/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=<script>alert(123)</script>; PHPSESSID=592pnf1jafdckauam7unlp9572;

date: Wed, 27 Sep 2023 05:34:48 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
set-cookie: PHPSESSID=592pnf1jafdckauam7unlp9572; path=/; HttpOnly,security=impossible; HttpOnly
content-length: 4428
keep-alive: timeout=5, max=12
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

```
="clear">
		</div>

		<div id="system_info">
			<input type="button" value="View Help" class="popup_button" id='help_button' data-help-url='../../vulnerabilities/view_help.php?id=sqli&security=<script>alert(123)</script>' )"> <input type="button" value="View Source" class="popup_button" id='source_button' data-source-url='../../vulnerabilities/view_source.php?id=sqli&security=

' )"> <input type="button" value="View Source" class="popup_button" id='source_button' data-source-url='../../vulnerabilities/view_source.php?id=sqli&security=<script>alert(123)</script>' )"> <div align="left"><em>Username:</em> admin<br /><em>Security Level:</em> impossible<br /><em>PHPIDS:</em> disabled</div>
		</div>

		<div id="footer">

			<p>Damn Vulnerable Web Applicat
```

Url: http://localhost/dvwa/vulnerabilities/sqli_blind/?id='&Submit=Submit
Occurrences in this Url: 1

Request

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/vulnerabilities/sqli_blind/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=<script>alert(123)</script>;
PHPSESSID=592pnf1jafdckauam7unlp9572;
```

Response

```
date: Wed, 27 Sep 2023 05:34:50 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
set-cookie: PHPSESSID=592pnf1jafdckauam7unlp9572;
path=/; HttpOnly,security=impossible; HttpOnly
content-length: 4590
keep-alive: timeout=5, max=28
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

r">
        </div>

        <div id="system_info">
            <input type="button" value="View Help" class="popup_button" id='help_button' data-help-url='../../vulnerabilities/view_help.php?id=sqli_blind&security=<script>alert(123)</script>' )"> <input type="button" value="View Source" class="popup_button" id='source_button' data-source-url='../../vulnerabilities/view_source.php?id=sqli_blind&security=<span class="vulnerabilities_highli

' )"> <input type="button" value="View Source" class="popup_button" id='source_button' data-source-url='../../vulnerabilities/view_source.php?id=sqli_blind&security=<script>alert(123)</script>' )"> <div align="left"><em>Username:</em> admin<br /><em>Security Level:</em> impossible<br /><em>PHPIDS:</em> disabled</div>
        </div>

        <div id="footer">

            <p>Damn Vulnerable Web Applicat
```

Url: http://localhost/dvwa/vulnerabilities/xss_r
Occurrences in this Url: 1

Request

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
```

Response

```
date: Wed, 27 Sep 2023 05:34:52 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
set-cookie: PHPSESSID=592pnf1jafdckauam7unlp9572;
```

```
referer: http://localhost/dvwa/vulnerabilities/sqli_blind/?id=%27&Submit=Submit
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=<script>alert(123)</script>;
PHPSESSID=592pnf1jafdckauam7unlp9572;
```

```
path=/; HttpOnly,security=impossible; HttpOnly
content-length: 4334
keep-alive: timeout=5, max=9
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

"clear">
            </div>

            <div id="system_info">
                <input type="button" value="View Help" class="popup_button" id='help_button' data-help-url='../../vulnerabilities/view_help.php?id=xss_r&security=<script>alert(123)</script>' )"> <input type="button" value="View Source" class="popup_button" id='source_button' data-source-url='../../vulnerabilities/view_source.php?id=xss_r&security=

' )"> <input type="button" value="View Source" class="popup_button" id='source_button' data-source-url='../../vulnerabilities/view_source.php?id=xss_r&security=<script>alert(123)</script>' )"> <div align="left"><em>Username:</em> admin<br /><em>Security Level:</em> impossible<br /><em>PHPIDS:</em> disabled</div>
            </div>

            <div id="footer">

                <p>Damn Vulnerable Web Applicat
```

Url: http://localhost/dvwa/vulnerabilities/xss_r/?name=123

Occurrences in this Url: 1

Request

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/vulnerabilities/xss_r/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=<script>alert(123)</script>;
PHPSESSID=592pnf1jafdckauam7unlp9572;
```

Response

```
date: Wed, 27 Sep 2023 05:34:53 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
set-cookie: PHPSESSID=592pnf1jafdckauam7unlp9572;
path=/; HttpOnly,security=impossible; HttpOnly
content-length: 4465
keep-alive: timeout=5, max=61
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

"clear">
            </div>
            <div id="system_info">
                <input type="button" value="View Help" class="popup_button" id='help_button' data-help-url='../../vulnerabilities/view_help.php?id=xss_r&security=<script>alert(123)</script>' )"> <input type="button" value="View Source" class="popup_button" id='source_button' data-source-url='../../vulnerabilities/view_source.php?id=xss_r&security=

' )"> <input type="button" value="View Source" class="popup_button" id='source_button' data-source-url='../../vulnerabilities/view_source.php?id=xss_r&security=<script>alert(123)</script>' )"> <div align="left"><em>Username:</em> admin<br /><em>Security Level:</em> impossible<br /><em>PHPIDS:</em> disabled</div>
            </div>

            <div id="footer">

                <p>Damn Vulnerable Web Applicat
```

Findings: 7 Verb tampering

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Medium	Medium	5.3	2

Description

Vooki has detected a HTTP verb tampering vulnerability in the URL http://localhost/dvwa/login.php.A 200 response status code indicates that the web server responded to the 'GET' method and returned some data when the request method was changed from POST to GET.
Reference:
https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/07-Input_Validation_Testing/03-Testing_for_HTTP_Verb_Tampering

Remediation

Make sure that only necessary and verified methods are accepted at server

Classification:	OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5, CWE: 650
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Url:	http://localhost/dvwa/login.php
Occurrences in this Url:	1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 content-type: application/x-www-form-urlencoded referer: http://localhost/dvwa/login.php origin: http://localhost upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=impossible; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:34:42 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 1415 keep-alive: timeout=5, max=48 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url:	http://localhost/dvwa/security.php
Occurrences in this Url:	1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 content-type: application/x-www-form-urlencoded referer: http://localhost/dvwa/security.php	date: Wed, 27 Sep 2023 05:34:45 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 5283 keep-alive: timeout=5, max=25 connection: Keep-Alive

```
origin: http://localhost
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=impossible;
PHPSESSID=592pnf1jafdckauam7unlp9572
```

```
content-type: text/html;charset=utf-8
status code: 200
```

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 8 Technical information exposure on the webpage

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Medium	Medium	5.3	2

Description

Vooki has identified technical information exposure on the webpage's URL http://localhost/dvwa/index.php. For POC references, look at the highlighted text in the response area. When an application fails to adequately safeguard technical, sensitive, and secret information from persons who shouldn't normally have access to the subject matter, information disclosure occurs.

Remediation

Delete any extraneous technical details from the website.

Classification:	OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5.8, CWE: 200
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Url:	http://localhost/dvwa/index.php
Occurrences in this Url:	2

Request

```
Method: GET
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate
referer: http://localhost/dvwa/login.php
connection: keep-alive
cookie: security=impossible; PHPSESSID=592pnf1jafdckauam7unlp9572
```

Response

```
date: Wed, 27 Sep 2023 05:30:14 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 6434
keep-alive: timeout=5, max=99
connection: Keep-Alive
content-type: text/html;charset=utf-8

> or <a href="https://www.vmware.com/" target="_blank">VMware</a>), which is set to NAT networking mode. Inside a guest machine, you can download and install <a href="https://www.apachefriends.org/en/xampp.html" target="_blank">

.html" target="_blank">XAMPP</a> for the web server and database.</p>
    <br />
    <h3>Disclaimer</h3>
    <p>We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the
```

Payloads and Evidence are highlighted in the red color

Findings: 9 Sensitive information disclosure in response headers - x-powered-by

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Medium	Medium	5.3	6

Description

Vooki has detected the 'x-powered-by' header from the response header of the URL http://localhost/dvwa. This discloses sensitive information. It might be useful for information gathering by unauthorized or 3rd party users with hacking prowess.

Remediation

Remove the 'x-powered-by' header from the server response. Ensure that your web server does not send out response headers or background information that reveals technical details about the back-end technology type, version, or setup.

Classification:	OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5, CWE: 212
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Url:	http://localhost/dvwa
Occurrences in this Url:	1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: cross-site connection: keep-alive	date: Wed, 27 Sep 2023 05:34:39 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 set-cookie: PHPSESSID=5k8pmj8rtv7633gf0uhj5g3sce; path=/,PHPSESSID=5k8pmj8rtv7633gf0uhj5g3sce; path=/; HttpOnly,security=impossible; HttpOnly expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 1415 keep-alive: timeout=5, max=90 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url:	http://localhost/dvwa/login.php
Occurrences in this Url:	1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 connection: keep-alive cookie: security=impossible; PHPSESSID=1klskcb5cr1o6aakt71rij3nbu	date: Wed, 27 Sep 2023 05:34:40 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 1415 keep-alive: timeout=5, max=74 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli

Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/security.php upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:34:47 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 4207 keep-alive: timeout=5, max=7 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/vulnerabilities/sqli/ upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:34:49 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache content-length: 162 keep-alive: timeout=5, max=53 connection: Keep-Alive content-type: text/html; charset=UTF-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli_blind/?id='&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/vulnerabilities/sqli_blind/ upgrade-insecure-requests: 1 sec-fetch-dest: document	date: Wed, 27 Sep 2023 05:34:51 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 4317 keep-alive: timeout=5, max=12 connection: Keep-Alive content-type: text/html;charset=utf-8

sec-fetch-site: same-origin

sec-fetch-user: ?1

connection: keep-alive

cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572

status code: 404

Url: http://localhost/dvwa/vulnerabilities/xss_r/?name=123

Occurrences in this Url: 1

Request

Method: GET

user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0

accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

accept-language: en-US,en;q=0.5

referer: http://localhost/dvwa/vulnerabilities/xss_r/

upgrade-insecure-requests: 1

sec-fetch-dest: document

sec-fetch-site: same-origin

sec-fetch-user: ?1

connection: keep-alive

cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572

Response

date: Wed, 27 Sep 2023 05:34:54 GMT

server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30

x-powered-by: PHP/7.4.30

expires: Tue, 23 Jun 2009 12:00:00 GMT

cache-control: no-cache, must-revalidate

pragma: no-cache

x-xss-protection: 0

content-length: 4214

keep-alive: timeout=5, max=28

connection: Keep-Alive

content-type: text/html;charset=utf-8

status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 10 Sensitive information disclosure in response headers - server

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Medium	Medium	5.3	6

Description

Vooki has detected the 'server' header from the response header of the URL http://localhost/dvwa. This discloses sensitive information. It might be useful for information gathering by unauthorized or 3rd party users with hacking prowess.

Remediation

Remove the 'server' header from the server response. Ensure that your web server does not send out response headers or background information that reveals technical details about the back-end technology type, version, or setup.

Classification:	OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5, CWE: 212
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Url: http://localhost/dvwa
Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: cross-site connection: keep-alive	date: Wed, 27 Sep 2023 05:34:39 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 set-cookie: PHPSESSID=5k8pmj8rtv7633gf0uhj5g3sce; path=/,PHPSESSID=5k8pmj8rtv7633gf0uhj5g3sce; path=/; HttpOnly,security=impossible; HttpOnly expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 1415 keep-alive: timeout=5, max=90 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url: http://localhost/dvwa/login.php
Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 connection: keep-alive cookie: security=impossible; PHPSESSID=1klskcb5cr1o6aakt71rij3nbu	date: Wed, 27 Sep 2023 05:34:40 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 1415 keep-alive: timeout=5, max=74 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli

Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/security.php upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:34:47 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 4207 keep-alive: timeout=5, max=7 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/vulnerabilities/sqli/ upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:34:49 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache content-length: 162 keep-alive: timeout=5, max=53 connection: Keep-Alive content-type: text/html; charset=UTF-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli_blind/?id='&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/vulnerabilities/sqli_blind/ upgrade-insecure-requests: 1 sec-fetch-dest: document	date: Wed, 27 Sep 2023 05:34:51 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 4317 keep-alive: timeout=5, max=12 connection: Keep-Alive content-type: text/html;charset=utf-8

```
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572
```

```
status code: 404
```

Url: http://localhost/dvwa/vulnerabilities/xss_r/?name=123

Occurrences in this Url: 1

Request

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/vulnerabilities/xss_r/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572
```

Response

```
date: Wed, 27 Sep 2023 05:34:54 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
x-xss-protection: 0
content-length: 4214
keep-alive: timeout=5, max=28
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200
```

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 11 Error Messages Detected

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Medium	Medium	5.3	1

Description

Vooki identified application error messages in the URL http://localhost/dvwa/vulnerabilities/sqli/?id=%27&Submit=<script>alert(123)</script>. This information can provide important clues on potential flaws in the site.

Remediation

- A precise error-handling policy should be created, including the sorts of errors that need to be handled, what information will be communicated back to the user, and what information will be logged.
- Make sure the program is designed to gracefully handle all potential problems. The program should respond to problems with a specially crafted outcome that is beneficial to the user without disclosing unneeded internal information.

Classification:	OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5, CWE: 703
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Url:	http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=<script>alert(123)</script>
Occurrences in this Url:	1

Request

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/vulnerabilities/sqli/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572
```

Response

```
date: Wed, 27 Sep 2023 05:34:48 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate
pragma: no-cache
content-length: 162
keep-alive: timeout=5, max=94
connection: Keep-Alive
content-type: text/html; charset=UTF-8
status code: 200

<pre>You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''''' at line 1</pre>
```

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 12 Possible Cross-Site Request Forgery Attack Detected

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	1

Description

Vooki identified the possibility of Cross site request forgery (CSRF) in the URL http://localhost/dvwa/login.php. Cross-site request forgery (CSRF) is a web security flaw that allows an attacker to trick users into performing actions they do not intend to perform.
Reference:
https://owasp.org/www-community/attacks/csrf

Remediation

- Implement an anti-CSRF token in all sensitive forms on authenticated pages.
- Use Built-in or existing CSRF implementations for CSRF protection.

.
Reference
https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

Classification:	OWASP 2021: A1, OWASP 2017: A5, OWASP API 2019: API5, PCI-DSS: 3.2.1-6.5.9, CWE: 352
CVSS Vector:	AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Url:	http://localhost/dvwa/login.php
Occurrences in this Url:	1

Request	Response
Method: POST	date: Wed, 27 Sep 2023 05:34:54 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 set-cookie: PHPSESSID=s2tj3h9l4ij56irnd74siaphjp; path=/,PHPSESSID=s2tj3h9l4ij56irnd74siaphjp; path=/; HttpOnly,security=impossible; HttpOnly expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 1415 keep-alive: timeout=5, max=94 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 13 Missing security headers - X-Frame-Options

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	5

Description

Vooki found out that the URL http://localhost/dvwa is missing the X-Frame-Options security header. Your application can use certain HTTP response headers to make it more secure. Once these HTTP response headers are set, they can stop modern browsers from encountering easily avoidable vulnerabilities.

X-Frame-Options: The 'X-Frame-Options' HTTP response header can be used to indicate whether browsers should be allowed to render a page in a <frame>, <iframe>, <embed>, or <object>.

Values of 'X-Frame-Options' header:
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN

DENY: If 'X-Frame-Options: DENY' is specified, the page cannot be displayed in a frame, regardless of the site attempting to do so.
SAMEORIGIN: If 'X-Frame-Options: SAMEORIGIN' is specified, the page can only be displayed in a frame on the same origin as the page itself.

Remediation

It is advised to use the 'X-Frame-Options' security header with the value 'deny' or'sameorigin'.
Reference
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#xcto

Classification: OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5, CWE: 693
CVSS Vector: AV:N/AC:H/Au:N/C:P/I:N/A:N

Url: http://localhost/dvwa
Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: cross-site connection: keep-alive	date: Wed, 27 Sep 2023 05:34:39 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 set-cookie: PHPSESSID=184ae48mni3q42ftnt8rengi6t; path=/,PHPSESSID=184ae48mni3q42ftnt8rengi6t; path=/; HttpOnly,security=impossible; HttpOnly expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 1415 keep-alive: timeout=5, max=88 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url: http://localhost/dvwa/login.php
Occurrences in this Url: 1

Request	Response
Method: GET	date: Wed, 27 Sep 2023 05:34:41 GMT

```
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
connection: keep-alive
cookie: security=impossible; PHPSESSID=1klskcb5cr1o6aakt71rij3nbu
```

```
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 1415
keep-alive: timeout=5, max=73
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200
```

Url: http://localhost/dvwa/vulnerabilities/sqli

Occurrences in this Url: 1

Request

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/security.php
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572
```

Response

```
date: Wed, 27 Sep 2023 05:34:47 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 4207
keep-alive: timeout=5, max=15
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200
```

Url: http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit

Occurrences in this Url: 1

Request

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/vulnerabilities/sqli/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572
```

Response

```
date: Wed, 27 Sep 2023 05:34:49 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate
pragma: no-cache
content-length: 162
keep-alive: timeout=5, max=52
connection: Keep-Alive
content-type: text/html; charset=UTF-8
status code: 200
```

Url: http://localhost/dvwa/vulnerabilities/xss_r/?name=123

Occurrences in this Url: 1

Request

Response

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/vulnerabilities/xss_r/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572
```

```
date: Wed, 27 Sep 2023 05:34:54 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
x-xss-protection: 0
content-length: 4214
keep-alive: timeout=5, max=65
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200
```

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 14 Missing security headers - X-Content-Type-Options

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	5

Description

Vooki found out that the URL http://localhost/dvwa is missing the X-Content-Type-Options security header. Your application can use certain HTTP response headers to make it more secure. Once these HTTP response headers are set, they can stop modern browsers from encountering easily avoidable vulnerabilities.

The X-Content-Type-Options response header is used by the server to signal that the MIME types indicated in the Content-Type headers should be followed and not modified. The header prevents MIME type snooping by stating that the MIME types are purposefully defined. The header can contain two values: nosniff and none.

Example: X-Content-Type-Options: nosniff
If 'X-Content-Type-Options: nosniff' is specified in the response header, the browser checks the content type and blocks the request if the content type is mismatched.

Remediation

It is advised to use the 'X-Content-Type-Options' security header with the value nosniff.
Reference
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#xcto

Classification:	OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5, CWE: 693
CVSS Vector:	AV:N/AC:H/Au:N/C:P/I:N/A:N

Url:	http://localhost/dvwa
Occurrences in this Url:	1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: cross-site connection: keep-alive	date: Wed, 27 Sep 2023 05:34:39 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 set-cookie: PHPSESSID=184ae48mni3q42ftnt8rengi6t; path=/,PHPSESSID=184ae48mni3q42ftnt8rengi6t; path=/; HttpOnly,security=impossible; HttpOnly expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 1415 keep-alive: timeout=5, max=88 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url:	http://localhost/dvwa/login.php
Occurrences in this Url:	1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept:	date: Wed, 27 Sep 2023 05:34:41 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 connection: keep-alive cookie: security=impossible; PHPSESSID=1klskcb5cr1o6aakt71rij3nbu	cache-control: no-cache, must-revalidate pragma: no-cache content-length: 1415 keep-alive: timeout=5, max=73 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli

Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/security.php upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:34:47 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 4207 keep-alive: timeout=5, max=15 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/vulnerabilities/sqli/ upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:34:49 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache content-length: 162 keep-alive: timeout=5, max=52 connection: Keep-Alive content-type: text/html; charset=UTF-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/xss_r/?name=123

Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;	date: Wed, 27 Sep 2023 05:34:54 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30

```
rv:95.0) Gecko/20100101 Firefox/95.0
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/vulnerabilities/xss_r/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low;
PHPSESSID=592pnf1jafdckauam7unlp9572
```

```
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
x-xss-protection: 0
content-length: 4214
keep-alive: timeout=5, max=65
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200
```

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 15 Missing Content Security Policy in response header

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	6

Description

Vooki found out that the URL http://localhost/dvwa is missing the Content Security Policy header. Your application can use certain HTTP response headers to make it more secure. Once these HTTP response headers are set, they can stop modern browsers from encountering easily avoidable vulnerabilities.It's an extra layer of protection that aids in the detection and mitigation of data injection and Cross Site Scripting (XSS) vulnerabilities.

Remediation

It's recommended to include the Content Security Policy (CSP) header in the HTTP response.
Reference
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

Classification:	OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5, CWE: 693
CVSS Vector:	AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Url:	http://localhost/dvwa
Occurrences in this Url:	1

Request	Response
Method: GET	date: Wed, 27 Sep 2023 04:28:02 GMT
host: localhost	server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0	location: http://localhost/dvwa/
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	content-length: 330
accept-language: en-US,en;q=0.5	keep-alive: timeout=5, max=100
accept-encoding: gzip, deflate	connection: Keep-Alive
upgrade-insecure-requests: 1	content-type: text/html; charset=iso-8859-1
sec-fetch-dest: document	
sec-fetch-mode: navigate	
sec-fetch-site: cross-site	
connection: keep-alive	

Url:	http://localhost/dvwa/login.php
Occurrences in this Url:	1

Request	Response
Method: GET	date: Wed, 27 Sep 2023 04:28:03 GMT
host: localhost	server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0	x-powered-by: PHP/7.4.30
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	expires: Tue, 23 Jun 2009 12:00:00 GMT
accept-language: en-US,en;q=0.5	cache-control: no-cache, must-revalidate
accept-encoding: gzip, deflate	pragma: no-cache
connection: keep-alive	content-length: 1415
	keep-alive: timeout=5, max=98
	connection: Keep-Alive
	content-type: text/html;charset=utf-8

cookie: security=impossible; PHPSESSID=1klskcb5cr1o6aakt71rij3nbu

Url:	http://localhost/dvwa/vulnerabilities/sqli
Occurrences in this Url:	1

Request	Response
Method: GET host: localhost user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 accept-encoding: gzip, deflate referer: http://localhost/dvwa/security.php upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-mode: navigate sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:30:46 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 4207 keep-alive: timeout=5, max=100 connection: Keep-Alive content-type: text/html;charset=utf-8

Url:	http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit
Occurrences in this Url:	1

Request	Response
Method: GET host: localhost user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 accept-encoding: gzip, deflate referer: http://localhost/dvwa/vulnerabilities/sqli/ upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-mode: navigate sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:31:50 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache content-length: 162 keep-alive: timeout=5, max=100 connection: Keep-Alive content-type: text/html; charset=UTF-8

Url:	http://localhost/dvwa/vulnerabilities/sqli_blind/?id='&Submit=Submit
Occurrences in this Url:	1

Request	Response
Method: GET host: localhost	date: Wed, 27 Sep 2023 05:32:12 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30

```
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate
referer: http://localhost/dvwa/vulnerabilities/sqli_blind/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-mode: navigate
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572
```

```
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 4317
keep-alive: timeout=5, max=100
connection: Keep-Alive
content-type: text/html;charset=utf-8
```

Url:	http://localhost/dvwa/vulnerabilities/xss_r/?name=123
Occurrences in this Url:	1

Request

```
Method: GET
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate
referer: http://localhost/dvwa/vulnerabilities/xss_r/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-mode: navigate
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572
```

Response

```
date: Wed, 27 Sep 2023 05:32:45 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
x-xss-protection: 0
content-length: 4214
keep-alive: timeout=5, max=100
connection: Keep-Alive
content-type: text/html;charset=utf-8
```

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 16 HTTP trace support detected

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	1

Description

Vooki has detected that the HTTP TRACE method has been enabled in the application's URL http://localhost/dvwa. TRACE method allows the client to see what's being received at the other end of the request chain. This technique is intended for diagnostic use. However, Cross-Site Tracing (XST) may result from this.

Remediation

It is preferable to disable the TRACE technique unless absolutely essential even though it is not a susceptible action.

Classification:	OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5, CWE: 670
CVSS Vector:	AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Url:	http://localhost/dvwa
Occurrences in this Url:	1

Request

```
Method: TRACE
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: cross-site
connection: keep-alive
```

Response

```
date: Wed, 27 Sep 2023 05:34:40 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
keep-alive: timeout=5, max=83
connection: Keep-Alive
transfer-encoding: chunked
content-type: message/http
status code: 200
```

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 17 Autocomplete on sensitive fields

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	1

Description

Vooki has detected a vulnerability in the URL http://localhost/dvwa/login.php where autocomplete is enabled on sensitive fields. Autocomplete is a feature that allows the browser to remember values entered by the user in form fields and suggest them for future use. Autocomplete can be enabled or disabled for specific form fields using the autocomplete attribute.

Remediation

It is advised that autocomplete be turned off for all sensitive fields such as passwords, credit card numbers, social security numbers, and so on. For example: <input type='password' autocomplete='off' name='passw'>

Classification:	OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5, CWE: 16
CVSS Vector:	AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Url:	http://localhost/dvwa/login.php
Occurrences in this Url:	1

Request

```
Method: GET
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:95.0) Gecko/20100101 Firefox/95.0
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate
connection: keep-alive
cookie: security=impossible;
PHPSESSID=1klskcb5cr1o6aakt71rij3nbu
```

Response

```
date: Wed, 27 Sep 2023 04:28:03 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 1415
keep-alive: timeout=5, max=98
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

logo.png"></p>

    <br>

   </div>

   <div id="content">

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

     <fieldset>

      <label for="user">Username</label> <input type="te
xt" class="loginInput" size="20" name="username"><br>


      <label for="pass">Password</label> <input type="pa
ssword" class="loginInput" AUTOCOMPLETE="off" size="2
0" name="password"><br>
```

<br>

<p class="submit

Payloads and Evidence are highlighted in the red color

Findings: 18 Autocomplete on password fields

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	1

Description

Vooki has detected a vulnerability in the URL http://localhost/dvwa/login.php where autocomplete is enabled on password field. Autocomplete is a feature that allows the browser to remember values entered by the user in form fields and suggest them for future use. Autocomplete can be enabled or disabled for specific form fields using the autocomplete attribute.

Remediation

It is advised that autocomplete be turned off for all sensitive fields such as passwords, credit card numbers, social security numbers, and so on. For example: <input type='password' autocomplete='off' name='passw'>

Classification:	OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5, CWE: 16
CVSS Vector:	AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Url:	http://localhost/dvwa/login.php
Occurrences in this Url:	1

Request

```
Method: GET
host: localhost
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate
connection: keep-alive
cookie: security=impossible; PHPSESSID=1klskcb5cr1o6aakt71rij3nbu
```

Response

```
date: Wed, 27 Sep 2023 04:28:03 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 1415
keep-alive: timeout=5, max=98
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

st">

		<fieldset>

			<label for="user">Username</label> <input type="text" class="loginInput" size="20" name="username"><br>


			<label for="pass">Password</label> <input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password"><br>

			<br>

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

		</fieldset>
```

```
< input type='hidden' name='user_token' value='4f812
```

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 19 Missing security headers - X-XSS-Protection

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Information	Information	NA	4

Description

Vooki found out that the URL http://localhost/dvwa is missing the X-XSS-Protection security header. Your application can use certain HTTP response headers to make it more secure. Once these HTTP response headers are set, they can stop modern browsers from encountering easily avoidable vulnerabilities.

X-XSS-Protection: The X-XSS-Protection is a HTTP header that is designed to enable the cross-site scripting (XSS) filter built into modern web browsers. It stops pages from loading when they detect reflected cross-site scripting (XSS) attacks.

For example:
X-XSS-Protection: 1
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1;report=<reporting-URL>

Remediation

It's highly recommended to properly implement the 'X-XSS-Protection' security header.
Reference
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#xcto

Classification:	NA
CVSS Vector:	NA

Url:	http://localhost/dvwa
Occurrences in this Url:	1

Request

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: cross-site
connection: keep-alive
```

Response

```
date: Wed, 27 Sep 2023 05:34:39 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
set-cookie: PHPSESSID=184ae48mni3q42ftnt8rengi6t; path=/,PHPSESSID=184ae48mni3q42ftnt8rengi6t; path=/; HttpOnly,security=impossible; HttpOnly
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 1415
keep-alive: timeout=5, max=88
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200
```

Url:	http://localhost/dvwa/login.php
Occurrences in this Url:	1

Request

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept:
```

Response

```
date: Wed, 27 Sep 2023 05:34:41 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
```

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
connection: keep-alive
cookie: security=impossible; PHPSESSID=1klskcb5cr1o6aakt71rij3nbu

cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 1415
keep-alive: timeout=5, max=73
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli
Occurrences in this Url: 1

Request

Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/security.php
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572

Response

date: Wed, 27 Sep 2023 05:34:47 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 4207
keep-alive: timeout=5, max=15
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit
Occurrences in this Url: 1

Request

Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/vulnerabilities/sqli/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572

Response

date: Wed, 27 Sep 2023 05:34:49 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate
pragma: no-cache
content-length: 162
keep-alive: timeout=5, max=52
connection: Keep-Alive
content-type: text/html; charset=UTF-8
status code: 200

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 20 Missing header - Permissions-Policy

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Information	Information	NA	5

Description

Vooki has detected that the permission policy isn't implemented in this application. This specification defines a mechanism that allows developers to selectively enable and disable the use of various browser features and API's.

Remediation

It is suggested that a permission policy security header be used.
Reference
https://www.w3.org/TR/permissions-policy-1/ https://www.permissionspolicy.com/

Classification:	NA
CVSS Vector:	NA

Url:	http://localhost/dvwa
Occurrences in this Url:	1

Request

Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: cross-site
connection: keep-alive

Response

date: Wed, 27 Sep 2023 05:34:39 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
set-cookie: PHPSESSID=184ae48mni3q42ftnt8rengi6t; path=/,PHPSESSID=184ae48mni3q42ftnt8rengi6t; path=/; HttpOnly,security=impossible; HttpOnly
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 1415
keep-alive: timeout=5, max=88
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

Url:	http://localhost/dvwa/login.php
Occurrences in this Url:	1

Request

Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
connection: keep-alive
cookie: security=impossible; PHPSESSID=1klskcb5cr1o6aakt71rij3nbu

Response

date: Wed, 27 Sep 2023 05:34:41 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 1415
keep-alive: timeout=5, max=73
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli
Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/security.php upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:34:47 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 4207 keep-alive: timeout=5, max=15 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit
Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/vulnerabilities/sqli/ upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:34:49 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache content-length: 162 keep-alive: timeout=5, max=52 connection: Keep-Alive content-type: text/html; charset=UTF-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/xss_r/?name=123
Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/vulnerabilities/xss_r/ upgrade-insecure-requests: 1 sec-fetch-dest: document	date: Wed, 27 Sep 2023 05:34:54 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache x-xss-protection: 0 content-length: 4214 keep-alive: timeout=5, max=65 connection: Keep-Alive

```
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low;
PHPSESSID=592pnf1jafdckauam7unlp9572
```

```
content-type: text/html;charset=utf-8
status code: 200
```

ⓘ Payloads and Evidence are highlighted in the red color

Findings: 21 Missing header - Expect-CT

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Information	Information	NA	5

Description

Vooki has detected that the Expect-CT header is missing. The Expect-CT header lets sites opt in to reporting and enforcing Certificate Transparency requirements in order to prevent the use of unissued certificates for that site from going unnoticed.

Remediation

It is suggested that the Expect-CT security header be used. The Expect-CT header is not necessary if your certificate supports Signed Certificate Timestamp by default.
Reference
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Expect-CT

Classification:	NA
CVSS Vector:	NA

Url:	http://localhost/dvwa
Occurrences in this Url:	1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: cross-site connection: keep-alive	date: Wed, 27 Sep 2023 05:34:39 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 set-cookie: PHPSESSID=184ae48mni3q42ftnt8rengi6t; path=/,PHPSESSID=184ae48mni3q42ftnt8rengi6t; path=/; HttpOnly,security=impossible; HttpOnly expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 1415 keep-alive: timeout=5, max=88 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url:	http://localhost/dvwa/login.php
Occurrences in this Url:	1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 connection: keep-alive cookie: security=impossible; PHPSESSID=1klskcb5cr1o6aakt71rij3nbu	date: Wed, 27 Sep 2023 05:34:41 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 1415 keep-alive: timeout=5, max=73 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli
Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/security.php upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:34:47 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache content-length: 4207 keep-alive: timeout=5, max=15 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/sqli/?id='&Submit=Submit
Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/vulnerabilities/sqli/ upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-site: same-origin sec-fetch-user: ?1 connection: keep-alive cookie: security=low; PHPSESSID=592pnf1jafdckauam7unlp9572	date: Wed, 27 Sep 2023 05:34:49 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache content-length: 162 keep-alive: timeout=5, max=52 connection: Keep-Alive content-type: text/html; charset=UTF-8 status code: 200

Url: http://localhost/dvwa/vulnerabilities/xss_r/?name=123
Occurrences in this Url: 1

Request	Response
Method: GET user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 referer: http://localhost/dvwa/vulnerabilities/xss_r/ upgrade-insecure-requests: 1 sec-fetch-dest: document	date: Wed, 27 Sep 2023 05:34:54 GMT server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30 x-powered-by: PHP/7.4.30 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache x-xss-protection: 0 content-length: 4214 keep-alive: timeout=5, max=65 connection: Keep-Alive

```
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=low;
PHPSESSID=592pnf1jafdckauam7unlp9572
```

```
content-type: text/html;charset=utf-8
status code: 200
```

Payloads and Evidence are highlighted in the red color

Findings: 22 Direct dynamic code execution - eval injection

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Information	Information	NA	2

Description

Vooki has detected the direct dynamic code execution - eval injection vulnerability in the URL http://localhost/dvwa/security.php. Check the highlighted eval() in the response section.
The eval() function evaluates JavaScript code represented as a string. This function's eval() would execute any input that had not been validated if it had been provided..

Remediation

It is advised to either avoid using the eval() method or to check user input before providing it to the function.

Classification: NA
CVSS Vector: NA

Url: http://localhost/dvwa/security.php
Occurrences in this Url: 1

Request

```
Method: GET
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
referer: http://localhost/dvwa/index.php
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=impossible; PHPSESSID=592pnf1jafdckauam7unlp9572
```

Response

```
date: Wed, 27 Sep 2023 05:34:44 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 5283
keep-alive: timeout=5, max=40
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200

>You can enable PHPIDS across this site for the duration of your session.</p>

   <p>PHPIDS is currently: <em>disabled</em>. [<a href="?phpids=on">Enable PHPIDS</a>]</p>
   [<a href="?test=%22><script>eval(window.name)</script>">Simulate attack</a>] -
   [<a href="ids_log.php">View IDS log</a>]
</div>
            <br /><br />



         </div>

         <div class="clear">
         </div>

         <div id="system_info">
```

Url: http://localhost/dvwa/security.php

Occurrences in this Url: 1

Request

```
Method: POST
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
content-type: application/x-www-form-urlencoded
referer: http://localhost/dvwa/security.php
origin: http://localhost
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-site: same-origin
sec-fetch-user: ?1
connection: keep-alive
cookie: security=impossible; PHPSESSID=592pnf1jafdckauam7unlp9572
```

Response

```
date: Wed, 27 Sep 2023 05:34:46 GMT
server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
x-powered-by: PHP/7.4.30
expires: Tue, 23 Jun 2009 12:00:00 GMT
cache-control: no-cache, must-revalidate
pragma: no-cache
content-length: 5283
keep-alive: timeout=5, max=12
connection: Keep-Alive
content-type: text/html;charset=utf-8
status code: 200
```

```
>You can enable PHPIDS across this site for the duration of your session.</p>

    <p>PHPIDS is currently: <em>disabled</em>. [<a href="?phpids=on">Enable PHPIDS</a>]</p>
    [<a href="?test=%22><script>eval(window.name)</script>">Simulate attack</a>] -
    [<a href="ids_log.php">View IDS log</a>]
</div>
                <br /><br />



            </div>

            <div class="clear">
            </div>

            <div id="system_info">
```