Vooki Pro Version

Dynamic Application Security Testing Report

Target: New Request

VegaBird TECHNOLOGIES

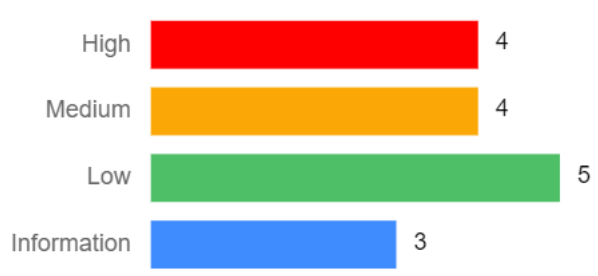
Scan information

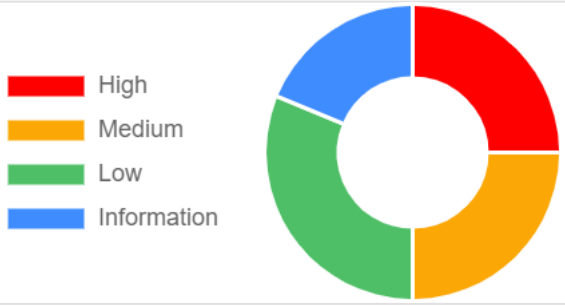
Target: New Request	Scan Type: API Scan
Scan Status: Completed	Report Type: Standard

Identified Vulnerabilities

IDENTIFIED	HIGH	MEDIUM	LOW	INFORMATION
16	4	4	5	3

Vulnerability Analysis





Vulnerability Findings

No	VULNERABILITY	RISK	SEVERITY	OCCURRENCES
1	Sql injection - MySQL	High	High	1
2	Insecure communication	High	High	1
3	Using Components with Known Vulnerabilities - Older version of PHP detected	High	High	1
4	Using Components with Known Vulnerabilities - Apache version 2.4.41	High	High	1
5	Sensitive information disclosure in response headers - x-powered-by	Medium	Medium	1
6	Sensitive information disclosure in response headers - server	Medium	Medium	1
7	Error Messages Detected	Medium	Medium	2
8	Missing security headers - X-Frame-Options	Low	Low	1
9	Missing security headers - X-Content-Type-Options	Low	Low	1
10	Missing Content Security Policy in response header	Low	Low	1
11	Insecure CORS	Low	Low	1
12	HTTP trace support detected	Low	Low	1
13	Missing security headers - X-XSS-Protection	Information	Information	1
14	Missing header - Permissions-Policy	Information	Information	1
15	Missing header - Expect-CT	Information	Information	1

Payloads and Evidence are highlighted in the red color

Findings: 1 Sql injection - MySQL

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
High	High	8.8	1

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 Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	date: Sun, 31 Jul 2022 10:09:27 GMT server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 x-powered-by: PHP/7.1.33 expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache access-control-allow-origin: * access-control-allow-headers: * content-length: 162 keep-alive: timeout=5, max=85 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 Insecure communication

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
High	High	7.5	1

Description

Vooki has detected an insecure communication vulnerability in the URL http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit. Insecure communications arise when a client and server communicate over a non-secure (unencrypted) channel. Without encrypting the channel, the developer can't guarantee the confidentiality and integrity of the data.

Remediation

Make sure all the client-to-server connections are encrypted with proper SSL certificate and validity.

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/vulnerabilities/sqli/?id=2&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	date: Sun, 31 Jul 2022 10:09:26 GMT server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 x-powered-by: PHP/7.1.33 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache access-control-allow-origin: * access-control-allow-headers: * content-length: 4545 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: 3 Using Components with Known Vulnerabilities - Older version of PHP detected

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
High	High	7.3	1

Description

VVooki has detected the php version (7.1.33) used in the URL http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit has known vulnerabilities as per the following vulnerability reference.
Reference:
https://www.php.net/eol.php

Remediation

Using a vulnerable php version isn't a good security practice and obviously isn't advisable. Hence, it's recommended to upgrade php to the latest version that's released in the market for safer security practices.

Classification: OWASP 2021: A6, OWASP 2017: A9, OWASP API 2019: API9, PCI-DSS: 3.2.1-6.2, CWE: 1035

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Url: http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit
Occurrences in this Url: 1

Request	Response
Method: GET	date: Sun, 31 Jul 2022 10:09:27 GMT
Cookie: security=low; _ga=GA1.1.676319044.1626240759;	server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33
security_level=0;	x-powered-by: PHP/7.1.33
PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	expires: Tue, 23 Jun 2009 12:00:00 GMT
	cache-control: no-cache, must-revalidate
	pragma: no-cache
	access-control-allow-origin: *
	access-control-allow-headers: *
	content-length: 4545
	keep-alive: timeout=5, max=90
	connection: Keep-Alive
	content-type: text/html;charset=utf-8
	status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 4 Using Components with Known Vulnerabilities - Apache version 2.4.41

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
High	High	7.3	1

Description

Vooki has detected the Apache version (2.4.41) used in the URL http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit has known vulnerabilities as per the following vulnerability reference.
Reference:
https://httpd.apache.org/security/vulnerabilities_24.html

Remediation

Using a vulnerable Apache version isn't a good security practice and obviously isn't advisable. Hence, it's recommended to upgrade Apache to the latest version that's released in the market for safer security practices.

Classification: OWASP 2021: A6, OWASP 2017: A9, OWASP API 2019: API9, PCI-DSS: 3.2.1-6.2, CWE: 1035

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Url: http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit
Occurrences in this Url: 1

Request	Response
Method: GET Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	date: Sun, 31 Jul 2022 10:09:27 GMT server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 x-powered-by: PHP/7.1.33 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache access-control-allow-origin: * access-control-allow-headers: * content-length: 4545 keep-alive: timeout=5, max=90 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 5 Sensitive information disclosure in response headers - x-powered-by

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Medium	Medium	5.3	1

Description

Vooki has detected the 'x-powered-by' header from the response header of the URL http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit. 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/vulnerabilities/sqli/?id=2&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	date: Sun, 31 Jul 2022 10:09:27 GMT server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 x-powered-by: PHP/7.1.33 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache access-control-allow-origin: * access-control-allow-headers: * content-length: 4545 keep-alive: timeout=5, max=90 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 6 Sensitive information disclosure in response headers - server

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Medium	Medium	5.3	1

Description

Vooki has detected the 'server' header from the response header of the URL http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit. 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/vulnerabilities/sqli/?id=2&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	date: Sun, 31 Jul 2022 10:09:27 GMT server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 x-powered-by: PHP/7.1.33 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache access-control-allow-origin: * access-control-allow-headers: * content-length: 4545 keep-alive: timeout=5, max=90 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 7 Error Messages Detected

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Medium	Medium	5.3	2

Description

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

Remediation

- A specific policy for handling errors should be implemented, including the types of errors to be handled, what information is going to be reported back to the user, and what information is going to be logged.
- Ensure that the application is built to handle all possible errors gracefully. When errors occur, the application should respond with a specifically designed result that is helpful to the user without revealing unnecessary internal details.

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=<script>alert('VOOKI-STORED-XSS')</script>&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	date: Sun, 31 Jul 2022 10:09:27 GMT server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 x-powered-by: PHP/7.1.33 expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache access-control-allow-origin: * access-control-allow-headers: * content-length: 187 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 'VOOKI-STORED-XSS')</script>'' at line 1</pre>

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

Occurrences in this Url: 1

Request	Response
Method: GET Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	date: Sun, 31 Jul 2022 10:09:27 GMT server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 x-powered-by: PHP/7.1.33 expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache

access-control-allow-origin: *

access-control-allow-headers: *

content-length: 162

keep-alive: timeout=5, max=85

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: 8 Missing security headers - X-Frame-Options

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	1

Description

Vooki has detected that X-Frame-Options security header is missing in the URL http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit. There are some HTTP response headers that your application can use to increase the security quality of your application. Once set, these HTTP response headers can restrict modern browsers from executing some easily preventable 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's recommended to implement the 'X-Frame-Options' security header with 'deny' or 'sameorigin' value.
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/vulnerabilities/sqli/?id=2&Submit=Submit
Occurrences in this Url: 1

Request	Response
Method: GET	date: Sun, 31 Jul 2022 10:09:27 GMT
Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33
	x-powered-by: PHP/7.1.33
	expires: Tue, 23 Jun 2009 12:00:00 GMT
	cache-control: no-cache, must-revalidate
	pragma: no-cache
	access-control-allow-origin: *
	access-control-allow-headers: *
	content-length: 4545
	keep-alive: timeout=5, max=87
	connection: Keep-Alive
	content-type: text/html;charset=utf-8
	status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 9 Missing security headers - X-Content-Type-Options

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	1

Description

Vooki has detected that 'X-Content-Type-Options' security header is missing in the URL http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit. There are some HTTP response headers that your application can use to increase the security posture of your application. Once set, these HTTP response headers can restrict modern browsers from executing some easily preventable vulnerabilities.

The 'X-Content-Type-Options' response HTTP header indicates the browser that the MIME types in the Content-Type headers shouldn't be changed and be followed.

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's recommended to implement the 'X-Content-Type-Options' security header.

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/vulnerabilities/sqli/?id=2&Submit=Submit
Occurrences in this Url: 1

Request	Response
Method: GET	date: Sun, 31 Jul 2022 10:09:27 GMT
Cookie: security=low; _ga=GA1.1.676319044.1626240759;	server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33
security_level=0;	x-powered-by: PHP/7.1.33
PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	expires: Tue, 23 Jun 2009 12:00:00 GMT
	cache-control: no-cache, must-revalidate
	pragma: no-cache
	access-control-allow-origin: *
	access-control-allow-headers: *
	content-length: 4545
	keep-alive: timeout=5, max=87
	connection: Keep-Alive
	content-type: text/html;charset=utf-8
	status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 10 Missing Content Security Policy in response header

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	1

Description

Vooki has detected that the Content Security Policy (CSP) is missing in the response header of the URL http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit. It's an added layer of security that helps to detect and mitigate data injection and Cross Site Scripting (XSS) vulnerabilities.

Remediation

It's recommended to include the Content Security Policy (CSP) header in the 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/vulnerabilities/sqli/?id=2&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET	date: Sun, 31 Jul 2022 10:09:26 GMT
Cookie: security=low; _ga=GA1.1.676319044.1626240759;	server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33
security_level=0;	x-powered-by: PHP/7.1.33
PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	expires: Tue, 23 Jun 2009 12:00:00 GMT
	cache-control: no-cache, must-revalidate
	pragma: no-cache
	access-control-allow-origin: *
	access-control-allow-headers: *
	content-length: 4545
	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: 11 Insecure CORS

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	1

Description

VVooki has detected an insecure CORS vulnerability in the response section of the highlighted URL http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit. Cross-Origin Resource Sharing (CORS) is an HTTP-header based mechanism that allows a server to instruct other origins from where a browser should permit loading of resources.

Remediation

- If the 'Access-Control-Allow-Origin' header value is set to *, it means that the website is permitted to accept resources from all origins.
- The server must pinpoint a domain in the value of the 'Access-Control-Allow-Origin' header.

Classification: OWASP 2021: A5, OWASP 2017: A6, OWASP API 2019: API7, PCI-DSS: 3.2.1-6.5, CWE: 942

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Url: http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	date: Sun, 31 Jul 2022 10:09:26 GMT server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 x-powered-by: PHP/7.1.33 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache access-control-allow-origin: * access-control-allow-headers: * content-length: 4545 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: 12 HTTP trace support detected

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	1

Description

Vooki has detected a HTTP TRACE in the application's URL http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit. TRACE method allows the client to see what's being received at the other end of the request chain. This method is designed for diagnostic purposes. But, this can lead to Cross-Site Tracing (XST).

Remediation

Enabling the TRACE method isn't a vulnerable activity, but it's better to disable it unless it's necessary.

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/vulnerabilities/sqli/?id=2&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: TRACE Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	date: Sun, 31 Jul 2022 10:09:53 GMT server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 keep-alive: timeout=5, max=56 connection: Keep-Alive transfer-encoding: chunked content-type: message/http status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 13 Missing security headers - X-XSS-Protection

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Information	Information	NA	1

Description

Vooki has detected that X-XSS-Protection security header is missing in the URL http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit. There are some HTTP response headers that your application can use to increase the security quality of your application. Once set, these HTTP response headers can restrict modern browsers from running into easily preventable vulnerabilities.

X-XSS-Protection: The HTTP 'X-XSS-Protection' response header is a mechanism that stops pages from loading when Internet Explorer, Chrome, and Safari 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 and configure 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/vulnerabilities/sqli/?id=2&Submit=Submit
Occurrences in this Url: 1

Request	Response
Method: GET Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	date: Sun, 31 Jul 2022 10:09:27 GMT server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 x-powered-by: PHP/7.1.33 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache access-control-allow-origin: * access-control-allow-headers: * content-length: 4545 keep-alive: timeout=5, max=87 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 header - Permissions-Policy

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Information	Information	NA	1

Description

Vooki has detected that the permission policy isn't implemented on 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's recommended to implement the permission policy security header.

Reference

https://www.w3.org/TR/permissions-policy-1/ https://www.permissionspolicy.com/

Classification: NA

CVSS Vector: NA

Url: http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	date: Sun, 31 Jul 2022 10:09:27 GMT server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 x-powered-by: PHP/7.1.33 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache access-control-allow-origin: * access-control-allow-headers: * content-length: 4545 keep-alive: timeout=5, max=87 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 header - Expect-CT

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Information	Information	NA	1

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's recommended to implement the Expect-CT security header. If your certificate supports Signed Certificate Timestamp by default, then the Expect-CT header isn't required.

Reference

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Expect-CT

Classification: NA

CVSS Vector: NA

Url: http://localhost/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit

Occurrences in this Url: 1

Request	Response
Method: GET Cookie: security=low; _ga=GA1.1.676319044.1626240759; security_level=0; PHPSESSID=tgissufd3tkpgn85ks2ivvkcu6	date: Sun, 31 Jul 2022 10:09:27 GMT server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 x-powered-by: PHP/7.1.33 expires: Tue, 23 Jun 2009 12:00:00 GMT cache-control: no-cache, must-revalidate pragma: no-cache access-control-allow-origin: * access-control-allow-headers: * content-length: 4545 keep-alive: timeout=5, max=87 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200