Vooki Pro Version

Dynamic Application Security Testing Report

Target: dvwa

VOOKI
INFOSEC

Scan information

Target
dvwa

Scan Type
API Scan

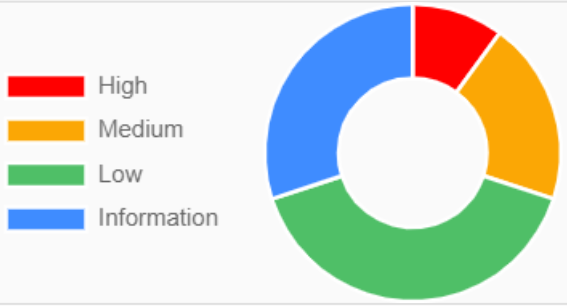
Scan Status
Completed

Report Type
Standard

Identified Vulnerabilities

IDENTIFIED	HIGH	MEDIUM	LOW	INFORMATION
10	1	2	4	3

Vulnerability Analysis



Vulnerability Findings

No	VULNERABILITY	RISK	SEVERITY	OCCURRENCES
1	Insecure communication detected	High	High	1
2	Sensitive information disclosure in response headers - x-powered-by	Medium	Medium	1
3	Sensitive information disclosure in response headers - server	Medium	Medium	1
4	Missing security headers - X-Frame-Options	Low	Low	1
5	Missing security headers - X-Content-Type-Options	Low	Low	1
6	Missing Content Security Policy in response header	Low	Low	1
7	HTTP trace support detected	Low	Low	1
8	Missing security headers - X-XSS-Protection	Information	Information	1
9	Missing header - Permissions-Policy	Information	Information	1
10	Missing header - Expect-CT	Information	Information	1

Payloads and Evidence are highlighted in the red color

Findings: 1 Insecure communication detected

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
High	High	7.5	1

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	Response
Method: GET Content-Type: application/json	date: Tue, 26 Sep 2023 12:25:12 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=2j7360n2a793pbavi93kka2da9; path=/,PHPSESSID=2j7360n2a793pbavi93kka2da9; 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=100 connection: Keep-Alive content-type: text/html;charset=utf-8 status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 2 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/login.php. 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/login.php
Occurrences in this Url: 1

Request	Response
Method: GET	date: Tue, 26 Sep 2023 12:25:13 GMT
Content-Type: application/json	server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
	x-powered-by: PHP/7.4.30
	set-cookie: PHPSESSID=n5npn79mg2qi0fvdde9cnao6u4; path=/,PHPSESSID=n5npn79mg2qi0fvdde9cnao6u4; 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=97
	connection: Keep-Alive
	content-type: text/html;charset=utf-8
	status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 3 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/login.php. 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/login.php
Occurrences in this Url: 1

Request	Response
Method: GET	date: Tue, 26 Sep 2023 12:25:13 GMT
Content-Type: application/json	server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
	x-powered-by: PHP/7.4.30
	set-cookie: PHPSESSID=n5npn79mg2qi0fvdde9cnao6u4; path=/,PHPSESSID=n5npn79mg2qi0fvdde9cnao6u4; 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=97
	connection: Keep-Alive
	content-type: text/html;charset=utf-8
	status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 4 Missing security headers - X-Frame-Options

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	1

Description

Vooki found out that the URL http://localhost/dvwa/login.php 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/login.php
Occurrences in this Url: 1

Request	Response
Method: GET	date: Tue, 26 Sep 2023 12:25:13 GMT
Content-Type: application/json	server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
	x-powered-by: PHP/7.4.30
	set-cookie: PHPSESSID=kalcp46anlg1ts8s1jtubbr0l3; path=/,PHPSESSID=kalcp46anlg1ts8s1jtubbr0l3; 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=96
	connection: Keep-Alive
	content-type: text/html;charset=utf-8
	status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 5 Missing security headers - X-Content-Type-Options

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	1

Description

Vooki found out that the URL http://localhost/dvwa/login.php 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/login.php
Occurrences in this Url: 1

Request	Response
Method: GET	date: Tue, 26 Sep 2023 12:25:13 GMT
Content-Type: application/json	server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
	x-powered-by: PHP/7.4.30
	set-cookie: PHPSESSID=kalcp46anlg1ts8s1jtubbr0l3; path=/,PHPSESSID=kalcp46anlg1ts8s1jtubbr0l3; 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=96
	connection: Keep-Alive
	content-type: text/html;charset=utf-8
	status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 6 Missing Content Security Policy in response header

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Low	Low	3.1	1

Description

Vooki found out that the URL http://localhost/dvwa/login.php 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/login.php
Occurrences in this Url: 1

Request	Response
Method: GET	date: Tue, 26 Sep 2023 12:25:12 GMT
Content-Type: application/json	server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
	x-powered-by: PHP/7.4.30
	set-cookie: PHPSESSID=2j7360n2a793pbavi93kka2da9;
	path=/,PHPSESSID=2j7360n2a793pbavi93kka2da9;
	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=100
	connection: Keep-Alive
	content-type: text/html;charset=utf-8

Payloads and Evidence are highlighted in the red color

Findings: 7 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/login.php. 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/login.php
Occurrences in this Url: 1

Request	Response
Method: TRACE	date: Tue, 26 Sep 2023 12:25:13 GMT
Content-Type: application/json	server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
	keep-alive: timeout=5, max=88
	connection: Keep-Alive
	transfer-encoding: chunked
	content-type: message/http
	status code: 200

Payloads and Evidence are highlighted in the red color

Findings: 8 Missing security headers - X-XSS-Protection

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Information	Information	NA	1

Description

Vooki found out that the URL http://localhost/dvwa/login.php 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/login.php
Occurrences in this Url: 1

Request	Response
Method: GET	date: Tue, 26 Sep 2023 12:25:13 GMT
Content-Type: application/json	server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
	x-powered-by: PHP/7.4.30
	set-cookie: PHPSESSID=kalcp46anlg1ts8s1jtubbr0l3; path=/,PHPSESSID=kalcp46anlg1ts8s1jtubbr0l3; 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=96
	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 header - Permissions-Policy

RISK	SEVERITY	CVSSv3 SCORE	OCCURRENCES
Information	Information	NA	1

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/login.php

Occurrences in this Url: 1

Request	Response
Method: GET	date: Tue, 26 Sep 2023 12:25:13 GMT
Content-Type: application/json	server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
	x-powered-by: PHP/7.4.30
	set-cookie: PHPSESSID=kalcp46anlg1ts8s1jtubbr0l3; path=/,PHPSESSID=kalcp46anlg1ts8s1jtubbr0l3; 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=96
	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 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 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/login.php

Occurrences in this Url: 1

Request	Response
Method: GET	date: Tue, 26 Sep 2023 12:25:13 GMT
Content-Type: application/json	server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
	x-powered-by: PHP/7.4.30
	set-cookie: PHPSESSID=kalcp46anlg1ts8s1jtubbr0l3; path=/,PHPSESSID=kalcp46anlg1ts8s1jtubbr0l3; 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=96
	connection: Keep-Alive
	content-type: text/html;charset=utf-8
	status code: 200