ZAP by Checkmarx Scanning Report

Generated with ZAP on Thu 17 Apr 2025, at 18:42:46

ZAP Version: 2.16.0

ZAP by Checkmarx

Contents

About this report

Report parameters

Contexts

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

Sites

The following sites were included:

- http://localhost:8080

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

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

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

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

Summaries

Alert counts by risk and confidence

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

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

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	1 (5.9%)	0 (0.0%)	1 (5.9%)
	Medium	0 (0.0%)	2 (11.8%)	2 (11.8%)	2 (11.8%)	6 (35.3%)
	Low	0 (0.0%)	1 (5.9%)	4 (23.5%)	0 (0.0%)	5 (29.4%)
	Informational	0 (0.0%)	2 (11.8%)	2 (11.8%)	1 (5.9%)	5 (29.4%)
	Total	0 (0.0%)	5 (29.4%)	9 (52.9%)	3 (17.6%)	17 (100%)

Alert counts by site and risk

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

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

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

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://localhost:8080	1 (1)	6 (7)	5 (12)	5 (17)

Alert counts by alert type

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

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

Alert type	Risk	Count
SQL Injection - MySQL	High	3 (17.6%)
Absence of Anti-CSRF Tokens	Medium	2 (11.8%)
Total		17

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	4 (23.5%)
Directory Browsing	Medium	1 (5.9%)
Hidden File Found	Medium	2 (11.8%)
Missing Anti-clickjacking Header	Medium	2 (11.8%)
Parameter Tampering	Medium	2 (11.8%)
Cookie No HttpOnly Flag	Low	1 (5.9%)
Cookie without SameSite Attribute	Low	1 (5.9%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	2 (11.8%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	5 (29.4%)
X-Content-Type-Options Header Missing	Low	3 (17.6%)
Authentication Request Identified	Informational	1 (5.9%)
GET for POST	Informational	1 (5.9%)
Total		17

Alert type	Risk	Count
Session Management Response Identified	Informational	3 (17.6%)
User Agent Fuzzer	Informational	12 (70.6%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	1 (5.9%)
Total		17

Alerts

Risk=High, Confidence=Medium (1)

http://localhost:8080 (1)

SQL Injection - MySQL (1)

▶ POST http://localhost:8080/secure/signin.php

Risk=Medium, Confidence=High (2)

http://localhost:8080 (2)

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

▶ GET http://localhost:8080/robots.txt

Hidden File Found (1)

▶ GET http://localhost:8080/server-status

Risk=Medium, Confidence=Medium (2)

http://localhost:8080 (2)

Directory Browsing (1)

▶ GET http://localhost:8080/secure/

Missing Anti-clickjacking Header (1)

▶ GET http://localhost:8080/secure/signin.php

Risk=Medium, Confidence=Low (2)

http://localhost:8080 (2)

Absence of Anti-CSRF Tokens (1)

▶ POST http://localhost:8080/secure/signin.php

Parameter Tampering (1)

▶ POST http://localhost:8080/secure/signin.php

Risk=Low, Confidence=High (1)

http://localhost:8080 (1)

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

▶ GET http://localhost:8080/secure/coding.jpeg

Risk=Low, Confidence=Medium (4)

http://localhost:8080 (4)

Cookie No HttpOnly Flag (1)

▶ GET http://localhost:8080/secure/signin.php

Cookie without SameSite Attribute (1)

▶ GET http://localhost:8080/secure/signin.php

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

▶ GET http://localhost:8080/secure/signin.php

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

▶ GET http://localhost:8080/secure/coding.jpeg

Risk=Informational, Confidence=High (2)

http://localhost:8080 (2)

Authentication Request Identified (1)

▶ POST http://localhost:8080/secure/signin.php

GET for POST (1)

▶ GET http://localhost:8080/secure/signin.php

Risk=Informational, Confidence=Medium (2)

http://localhost:8080 (2)

Session Management Response Identified (1)

▶ GET http://localhost:8080/secure/signin.php

User Agent Fuzzer (1)

▶ GET http://localhost:8080/secure

Risk=Informational, Confidence=Low (1)

http://localhost:8080 (1)

User Controllable HTML Element Attribute (Potential XSS) (1)

▶ POST http://localhost:8080/secure/signin.php

Appendix

Alert types

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

SQL Injection - MySQL

Source	raised by an active scanner (SQL Injection)
CWE ID	89
WASC ID	19

Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html ▪ https://cwe.mitre.org/data/definitions/352.html

Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy ▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

- https://www.w3.org/TR/CSP/
- https://w3c.github.io/webappsec-csp/
- https://web.dev/articles/csp
- https://caniuse.com/#feat=contentsecuritypolicy
- https://content-security-policy.com/

Directory Browsing

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

Hidden File Found

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

Missing Anti-clickjacking Header

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

Parameter Tampering

Source	raised by an active scanner (Parameter Tampering)
CWE ID	472
WASC ID	20

Cookie No HttpOnly Flag

Source	raised by a passive scanner (Cookie No HttpOnly Flag)
CWE ID	1004
WASC ID	13
Reference	▪ https://owasp.org/www-community/HttpOnly

Cookie without SameSite Attribute

Source	raised by a passive scanner (Cookie without SameSite Attribute)

CWE ID	1275
WASC ID	13
Reference	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

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

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

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

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	497
WASC ID	13

Reference	▪ https://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) ▪ https://www.troyhunt.com/shhh-dont-let-your-response-headers/

X-Content-Type-Options Header Missing

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

Authentication Request Identified

Source	raised by a passive scanner (Authentication Request Identified)
Reference	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

GET for POST

Source	raised by an active scanner (GET for POST)
CWE ID	16
WASC ID	20

Session Management Response Identified

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

User Agent Fuzzer

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

User Controllable HTML Element Attribute (Potential XSS)

Source	raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS))
CWE ID	20
WASC ID	20
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html