ZAP by Checkmarx Scanning Report

Generated with ZAP on Mon 29 Dec 2025, at 13:58:47

ZAP Version: 2.17.0

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:

- https://localhost
- http://localhost

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

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

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

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

Summaries

Alert Counts by Risk and Confidence

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

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

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (8.3%)	2 (16.7%)	0 (0.0%)	3 (25.0%)
	Low	0 (0.0%)	2 (16.7%)	3 (25.0%)	0 (0.0%)	5 (41.7%)
	Informational	0 (0.0%)	2 (16.7%)	2 (16.7%)	0 (0.0%)	4 (33.3%)
	Total	0 (0.0%)	5 (41.7%)	7 (58.3%)	0 (0.0%)	12 (100%)

Alert Counts by Site and Risk

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

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

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

Site	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://localhost	0 (0)	1 (1)	0 (1)	0 (1)
http://localhost	0 (0)	2 (2)	5 (7)	4 (11)

Alert Counts by Alert Type

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

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

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	5 (41.7%)
HTTP Only Site	Medium	1 (8.3%)
Missing Anti-clickjacking Header	Medium	5 (41.7%)
Cookie No HttpOnly Flag	Low	1 (8.3%)
Cookie without SameSite Attribute	Low	1 (8.3%)
In Page Banner Information Leak	Low	2 (16.7%)
Total		12

Alert type	Risk	Count
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	5 (41.7%)
X-Content-Type-Options Header Missing	Low	5 (41.7%)
Authentication Request Identified	Informational	1 (8.3%)
GET for POST	Informational	1 (8.3%)
Session Management Response Identified	Informational	2 (16.7%)
User Agent Fuzzer	Informational	5 (41.7%)
Total		12

Insights

This table shows information that is likely to be very relevant to you, but which is not related to vulnerabilities, or potentially even related to the application in question.

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP errors logged - see the zap.log file for details	1
Low	Warning		ZAP warnings logged - see the zap.log file for details	105
Low	Exceeded Low		Percentage of network failures	6 %
Info	Informational	http://localhost	Percentage of responses with status code 2xx	90 %

Level	Reason	Site	Description	Statistic
Info	Informational	http://localhost	Percentage of responses with status code 3xx	3 %
Info	Exceeded Low	http://localhost	Percentage of responses with status code 4xx	5 %
Info	Informational	http://localhost	Percentage of endpoints with content type image/png	10 %
Info	Informational	http://localhost	Percentage of endpoints with content type text/html	90 %
Info	Informational	http://localhost	Percentage of endpoints with method GET	80 %
Info	Informational	http://localhost	Percentage of endpoints with method POST	20 %
Info	Informational	http://localhost	Count of total endpoints	10
Info	Informational	https://localhost	Percentage of endpoints with method GET	100 %
Info	Informational	https://localhost	Count of total endpoints	1

Alerts

Risk=Medium, Confidence=High (1)

http://localhost (1)

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

▶ GET http://localhost/sitemap.xml

Risk=Medium, Confidence=Medium (2)

https://localhost (1)

HTTP Only Site (1)

▶ GET http://localhost/library_management_system/public/

http://localhost (1)

Missing Anti-clickjacking Header (1)

▶ GET http://localhost/library_management_system/public/login.php

Risk=Low, Confidence=High (2)

http://localhost (2)

In Page Banner Information Leak (1)

▶ GET http://localhost/sitemap.xml

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

▶ GET http://localhost/library_management_system/public/captcha.php

Risk=Low, Confidence=Medium (3)

http://localhost (3)

Cookie No HttpOnly Flag (1)

▶ GET http://localhost/library_management_system/public/

Cookie without SameSite Attribute (1)

▶ GET http://localhost/library_management_system/public/

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

▶ GET http://localhost/library_management_system/public/captcha.php

Risk=Informational, Confidence=High (2)

http://localhost (2)

Authentication Request Identified (1)

▶ POST http://localhost/library_management_system/public/login.php

GET for POST (1)

▶ GET http://localhost/library_management_system/public/login.php

Risk=Informational, Confidence=Medium (2)

http://localhost (2)

Session Management Response Identified (1)

▶ GET http://localhost/library_management_system/public/

User Agent Fuzzer (1)

▶ GET
http://localhost/library_management_system/public/captcha.php

Appendix

Alert Types

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

Content Security Policy (CSP) Header Not Set

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

HTTP Only Site

Source	raised by an active scanner (HTTP Only Site)
CWE ID	311
WASC ID	4
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html ▪ https://letsencrypt.org/

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/Reference/Headers/X-Frame-Options

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://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site

In Page Banner Information Leak

Source	raised by a passive scanner (In Page Banner Information Leak)
CWE ID	497
WASC ID	13
Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/

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