ZAP Scanning Report

Generated with ZAP on Wed 27 Nov 2024, at 17:03:57

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

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://127.0.0.1:8443

(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%)	1 (8.3%)	1 (8.3%)	0 (0.0%)	2 (16.7%)
	Medium	0 (0.0%)	1 (8.3%)	1 (8.3%)	1 (8.3%)	3 (25.0%)
	Low	0 (0.0%)	2 (16.7%)	1 (8.3%)	0 (0.0%)	3 (25.0%)
	Informational	0 (0.0%)	1 (8.3%)	2 (16.7%)	1 (8.3%)	4 (33.3%)
	Total	0 (0.0%)	5 (41.7%)	5 (41.7%)	2 (16.7%)	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.)

	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)

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
Cross Site Scripting (DOM Based)	High	1 (8.3%)
Cross Site Scripting (Reflected)	High	1 (8.3%)
Absence of Anti-CSRF Tokens	Medium	6 (50.0%)
Content Security Policy (CSP) Header Not Set	Medium	6 (50.0%)
Total		12

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	3 (25.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	7 (58.3%)
Strict-Transport-Security Header Not Set	Low	7 (58.3%)
X-Content-Type-Options Header Missing	Low	4 (33.3%)
Authentication Request Identified	Informational	1 (8.3%)
Modern Web Application	Informational	3 (25.0%)
Re-examine Cache-control Directives	Informational	4 (33.3%)
User Agent Fuzzer	Informational	12 (100.0%)
Total		12

Alerts

Risk=High, Confidence=High (1)

Risk=High, Confidence=Medium (1)

Risk=Medium, Confidence=High (1)

Risk=Medium, Confidence=Medium (1)

Risk=Medium, Confidence=Low (1)

Risk=Low, Confidence=High (2)

Risk=Low, Confidence=Medium (1)

Risk=Informational, Confidence=High (1)

Risk=Informational, Confidence=Medium (2)

Risk=Informational, Confidence=Low (1)

Appendix

Alert types

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

Cross Site Scripting (DOM Based)

Source	raised by an active scanner (Cross Site Scripting (DOM Based))
CWE ID	79
WASC ID	8
Reference	▪ https://owasp.org/www-community/attacks/xss/ ▪ https://cwe.mitre.org/data/definitions/79.html

Cross Site Scripting (Reflected)

Source	raised by an active scanner (Cross Site Scripting (Reflected))

CWE ID	79
WASC ID	8
Reference	▪ https://owasp.org/www-community/attacks/xss/ ▪ https://cwe.mitre.org/data/definitions/79.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/

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

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

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200
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/

Strict-Transport-Security Header Not Set

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	- https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html - https://owasp.org/www-community/Security_Headers - https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security - https://caniuse.com/stricttransportsecurity - https://datatracker.ietf.org/doc/html/rfc6797

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/

Modern Web Application

Source raised by a passive scanner (Modern Web Application)

Re-examine Cache-control Directives

Source raised by a passive scanner (Re-examine Cache-control Directives)

CWE ID 525

WASC ID 13

Reference
- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

- https://grayduck.mn/2021/09/13/cache-control-recommendations/

User Agent Fuzzer

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