ZAP Scanning Report

Generated with ✒ ZAP on Sat 17 Aug 2024, at 21:59:12

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Contents

- - Appendix

  - - Alert types

About this report

Report description

Escaneo de vulnerabilidades

Report parameters

Contexts

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

Sites

The following sites were included:

- `http://localhost:8080`
- `https://accounts.google.com`

(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%)	1 (25.0%)	1 (25.0%)
	Medium	0 (0.0%)	1 (25.0%)	0 (0.0%)	1 (25.0%)	2 (50.0%)
	Low	0 (0.0%)	0 (0.0%)	1 (25.0%)	0 (0.0%)	1 (25.0%)
	Informational	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Total	0 (0.0%)	1 (25.0%)	1 (25.0%)	2 (50.0%)	4 (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			
			Information al
High (= High)	Medium (>= Medium)	Low (>= Low)	Informa tional)

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
Cloud Metadata Potentially Exposed	High	1 (25.0%)
Content Security Policy (CSP) Header Not Set	Medium	3 (75.0%)
Hidden File Found	Medium	4 (100.0%)
X-Content-Type-Options Header Missing	Low	1 (25.0%)
Total		4

Alerts

Risk=High**, Confidence=**Low **(1)**

Risk=Medium**, Confidence=**High **(1)**

Risk=Medium**, Confidence=**Low **(1)**

Risk=Low**, Confidence=**Medium **(1)**

Appendix

Alert types

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

Cloud Metadata Potentially Exposed

Source	raised by an active scanner ([Cloud Metadata Potentially Exposed](#))
Reference	■ https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/

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/

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

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