Glowroot ZAP Scanning Report

Generated with ZAP on mer. 19 avr. 2023, at 15:53:19

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:4000

(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: Haut, Moyen, Faible, Pour information

Excluded: None

Confidence levels

Included: User Confirmed, Haut, Moyen, Faible

Excluded: User Confirmed, Haut, Moyen, Faible, Faux positif

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	Haut	Moyen	Faible	Total
Risk	Haut	0 (0,0 %)	1 (12,5 %)	0 (0,0 %)	0 (0,0 %)	1 (12,5 %)
	Moyen	0 (0,0 %)	1 (12,5 %)	1 (12,5 %)	1 (12,5 %)	3 (37,5 %)
	Faible	0 (0,0 %)	0 (0,0 %)	1 (12,5 %)	0 (0,0 %)	1 (12,5 %)
	Pour information	0 (0,0 %)	0 (0,0 %)	2 (25,0 %)	1 (12,5 %)	3 (37,5 %)
	Total	0 (0,0 %)	2 (25,0 %)	4 (50,0 %)	2 (25,0 %)	8 (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			
		Haut (= Haut)	Moyen (>= Moyen)	Faible (>= Faible)	Pour information (>= Pour information)
Site	http://localhost:4000	1 (1)	3 (4)	1 (5)	3 (8)

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 (basé DOM)	Haut	3 (37,5 %)
Absence de Jetons Anti-CSRF	Moyen	11 (137,5 %)
Content Security Policy (CSP) Header Not Set	Moyen	4 (50,0 %)
Missing Anti-clickjacking Header	Moyen	4 (50,0 %)
X-Content-Type-Options Header Missing	Faible	8 (100,0 %)
Information Disclosure - Suspicious Comments	Pour information	3 (37,5 %)
Modern Web Application	Pour information	4 (50,0 %)
User Agent Fuzzer	Pour information	48 (600,0 %)
Total		8

Alerts

Risk=Haut, Confidence=Haut (1)

http://localhost:4000 (1)

Cross Site Scripting (basé DOM) (1)

▶ GET http://localhost:4000/#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e

Risk=Moyen, Confidence=Haut (1)

http://localhost:4000 (1)

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

▶ GET http://localhost:4000

Risk=Moyen, Confidence=Moyen (1)

http://localhost:4000 (1)

Missing Anti-clickjacking Header (1)

▶ GET http://localhost:4000

Risk=Moyen, Confidence=Faible (1)

http://localhost:4000 (1)

Absence de Jetons Anti-CSRF (1)

▶ GET http://localhost:4000/scripts/scripts.7743bbcc.js

Risk=Faible, Confidence=Moyen (1)

http://localhost:4000 (1)

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

▶ GET http://localhost:4000

Risk=Pour information, Confidence=Moyen (2)

http://localhost:4000 (2)

Modern Web Application (1)

▶ GET http://localhost:4000

User Agent Fuzzer (1)

▶ GET http://localhost:4000/

Risk=Pour information, Confidence=Faible (1)

http://localhost:4000 (1)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost:4000/scripts/vendor-flame-graph.15e87631.js

Appendix

Alert types

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

Cross Site Scripting (basé DOM)

Source	raised by an active scanner (Cross Site Scripting (basé DOM))
CWE ID	79
WASC ID	8
Reference	▪ http://projects.webappsec.org/Cross-Site-Scripting ▪ http://cwe.mitre.org/data/definitions/79.html

Absence de Jetons Anti-CSRF

Source	raised by a passive scanner (Absence de Jetons Anti-CSRF)
CWE ID	352
WASC ID	9
Reference	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery ▪ http://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 ▪ http://www.w3.org/TR/CSP/ ▪ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html ▪ http://www.html5rocks.com/en/tutorials/security/content-security-policy/ ▪ http://caniuse.com/#feat=contentsecuritypolicy ▪ http://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

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	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx ▪ https://owasp.org/www-community/Security_Headers

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
WASC ID	13

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

User Agent Fuzzer

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