ZAP Scanning Report

Generated with ZAP on sáb 9 mar 2024, at 16:10:37

ZAP Version: 2.14.0

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:8079

(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: Alto, Médio, Baixo, Informativo

Excluded: None

Confidence levels

Included: User Confirmed, Alto, Médio, Baixo

Excluded: User Confirmed, Alto, Médio, Baixo, Falso Positivo

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	Alto	Médio	Baixo	Total
Risk	Alto	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
	Médio	0 (0,0%)	1 (33,3%)	0 (0,0%)	1 (33,3%)	2 (66,7%)
	Baixo	0 (0,0%)	0 (0,0%)	1 (33,3%)	0 (0,0%)	1 (33,3%)
	Informativo	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
	Total	0 (0,0%)	1 (33,3%)	1 (33,3%)	1 (33,3%)	3 (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			
		Alto (= Alto)	Médio (>= Médio)	Baixo (>= Baixo)	Informativo (>= Informativo)
Site	http://localhost:8079	0 (0)	2 (2)	1 (3)	0 (3)

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	Médio	3 (100,0%)
Hidden File Found	Médio	4 (133,3%)
O servidor vaza informações por meio dos campos de cabecalho de resposta HTTP "X-Powered-By"	Baixo	3 (100,0%)
Total		3

Alerts

Risk=Médio, Confidence=Alto (1)

http://localhost:8079 (1)

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

▶ GET http://localhost:8079/orders

Risk=Médio, Confidence=Baixo (1)

http://localhost:8079 (1)

Hidden File Found (1)

▶ GET http://localhost:8079/.hg

Risk=Baixo, Confidence=Médio (1)

http://localhost:8079 (1)

O servidor vaza informações por meio dos campos de cabecalho de resposta HTTP "X-Powered-By" (1)

▶ GET http://localhost:8079/sitemap.xml

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/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/

Hidden File Found

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

O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"

Source	raised by a passive scanner (O servidor vaza informações por meio dos campos de cabecalho de resposta HTTP "X-Powered-By")
CWE ID	200
WASC ID	13
Reference	• http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx • http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html