ZAP Scanning Report antes

Generated with ZAP on sáb. 15 jun. 2024, at 23:10:33

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:

- http://localhost:3000
- http://localhost:3001

(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%)	1 (14,3%)	0 (0,0%)	1 (14,3%)
	Médio	0 (0,0%)	1 (14,3%)	1 (14,3%)	0 (0,0%)	2 (28,6%)
	Baixo	0 (0,0%)	0 (0,0%)	2 (28,6%)	1 (14,3%)	3 (42,9%)
	Informativo	0 (0,0%)	0 (0,0%)	1 (14,3%)	0 (0,0%)	1 (14,3%)
	Total	0 (0,0%)	1 (14,3%)	5 (71,4%)	1 (14,3%)	7 (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)

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
Injeção SQL - MySQL	Alto	1 (14,3%)
CSP: Wildcard Directive	Médio	11 (157,1%)
Configuração Incorreta Entre Domínios	Médio	18 (257,1%)
Fraqueza de script entre sites (persistente na resposta JSON)	Baixo	1 (14,3%)
O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"	Baixo	18 (257,1%)
X-Content-Type-Options Header Missing	Baixo	7 (100,0%)
User Agent Fuzzer	Informativo	36 (514,3%)
Total		7

Alerts

Risk=Alto, Confidence=Médio (1)

Risk=Médio, Confidence=Alto (1)

Risk=Médio, Confidence=Médio (1)

Risk=Baixo, Confidence=Médio (2)

Risk=Baixo, Confidence=Baixo (1)

Risk=Informativo, Confidence=Médio (1)

Appendix

Alert types

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

Injeção SQL - MySQL

Source	raised by an active scanner (Injeção SQL)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)

CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Configuração Incorreta Entre Domínios

Source	raised by a passive scanner (Configuração Incorreta Entre Domínios)
CWE ID	264
WASC ID	14
Reference	▪ https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Fraqueza de script entre sites (persistente na resposta JSON)

Source	raised by an active scanner (Cross Site Scripting (Persistente))
CWE ID	79
WASC ID	8

Reference

- https://owasp.org/www-community/attacks/xss/
- https://cwe.mitre.org/data/definitions/79.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 cabeçalho de resposta HTTP "X-Powered-By")

CWE ID 200

WASC ID 13

Reference

- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework
- https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.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

User Agent Fuzzer

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