ZAP Scanning Report depois

Generated with ZAP on sáb. 15 jun. 2024, at 23:49:04

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%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
	Médio	0 (0,0%)	1 (16,7%)	1 (16,7%)	0 (0,0%)	2 (33,3%)
	Baixo	0 (0,0%)	0 (0,0%)	2 (33,3%)	0 (0,0%)	2 (33,3%)
	Informativo	0 (0,0%)	0 (0,0%)	2 (33,3%)	0 (0,0%)	2 (33,3%)
	Total	0 (0,0%)	1 (16,7%)	5 (83,3%)	0 (0,0%)	6 (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)

		Risk			
		Alto (= Alto)	Médio (>= Médio)	Baixo (>= Baixo)	Informativo (>= Informativo)
Site	http://localhost:3001	0 (0)	0 (0)	1 (1)	0 (1)

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
CSP: Wildcard Directive	Médio	11 (183,3%)
Configuração Incorreta Entre Domínios	Médio	15 (250,0%)
O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"	Baixo	15 (250,0%)
X-Content-Type-Options Header Missing	Baixo	4 (66,7%)
Divulgação de Informações - Comentários Suspeitos	Informativo	1 (16,7%)
User Agent Fuzzer	Informativo	12 (200,0%)
Total		6

Alerts

Risk=Médio, Confidence=Alto (1)

Risk=Médio, Confidence=Médio (1)

Risk=Baixo, Confidence=Médio (2)

http://localhost:3001 (1)

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

▶ GET http://localhost:3001

Risk=Informativo, Confidence=Médio (2)

Appendix

Alert types

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

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

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

Divulgação de Informações - Comentários Suspeitos

Source	raised by a passive scanner (Divulgação de Informações - Comentários Suspeitos)
CWE ID	200
WASC ID	13

User Agent Fuzzer

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