ZAP Scanning Report

Generated with ZAP on qua. 13 mar. 2024, at 23:24:49

ZAP Version: 2.14.0

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:

- `https://c0yb79yznl.execute-api.us-east-1.amazonaws.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: `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%)	2 (25,0%)	0 (0,0%)	0 (0,0%)	2 (25,0%)
	Médio	0 (0,0%)	0 (0,0%)	1 (12,5%)	0 (0,0%)	1 (12,5%)

Risk	**Baixo**	0 (0,0%)	1 (12,5%)	1 (12,5%)	1 (12,5%)	3 (37,5%)
	Informativo	0 (0,0%)	0 (0,0%)	1 (12,5%)	1 (12,5%)	2 (25,0%)
	Total	0 (0,0%)	3 (37,5%)	3 (37,5%)	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			
		Alto (= Alto)	**Médio (>= Médio)**	**Baixo (>= Baixo)**	**Informativo (>= Informativo)**
Site	**https://c0yb79yznl.execute-api.us-east-1.amazonaws.com**	2 (2)	1 (3)	3 (6)	2 (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
Injeção SQL	Alto	11 (137,5%)
Injeção SQL - SQLite	Alto	1 (12,5%)
Erro de Formato de String	Médio	2 (25,0%)
Fraqueza de script entre sites (persistente na resposta JSON)	Baixo	1 (12,5%)
Strict-Transport-Security Header Not Set	Baixo	21 (262,5%)
X-Content-Type-Options Header Missing	Baixo	16 (200,0%)
Re-examine Cache-control Directives	Informativo	16 (200,0%)
User Agent Fuzzer	Informativo	204 (2.550,0%)
Total		8

Alerts

Risk=Alto, Confidence=Alto (2)

https://c0yb79yznl.execute-api.us-east-1.amazonaws.com (2)

Injeção SQL (1)

▶ GET https://c0yb79yznl.execute-api.us-east-1.amazonaws.com/dev/v1/totem/order?status=WAITING_PAYMENT&status=RECEIVED%27+AND+%271%27%3D%271%27+--+&status=FINALIZED

Injeção SQL - SQLite (1)

▶ PUT https://c0yb79yznl.execute-api.us-east-1.amazonaws.com/dev/v1/administrative/product/65f255b65a8d773f94ba9fc6

Risk=Médio, Confidence=Médio (1)

https://c0yb79yznl.execute-api.us-east-1.amazonaws.com (1)

Erro de Formato de String (1)

▶ PUT https://c0yb79yznl.execute-api.us-east-1.amazonaws.com/dev/v1/administrative/category/65f2553e5a8d773f94ba9fc4

Risk=Baixo, Confidence=Alto (1)

https://c0yb79yznl.execute-api.us-east-1.amazonaws.com (1)

Strict-Transport-Security Header Not Set (1)

▶ DELETE https://c0yb79yznl.execute-api.us-east-1.amazonaws.com/dev/v1/administrative/category/65f2564d5a8d773f94ba9fc8

Risk=Baixo, Confidence=Médio (1)

https://c0yb79yznl.execute-api.us-east-1.amazonaws.com (1)

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

▶ GET https://c0yb79yznl.execute-api.us-east-1.amazonaws.com/dev/v1/administrative/category

Risk=Baixo, Confidence=Baixo (1)

https://c0yb79yznl.execute-api.us-east-1.amazonaws.com (1)

Fraqueza de script entre sites (persistente na resposta JSON) (1)

▶ GET https://c0yb79yznl.execute-api.us-east-1.amazonaws.com/dev/v1/administrative/product

Risk=Informativo, Confidence=Médio (1)

https://c0yb79yznl.execute-api.us-east-1.amazonaws.com (1)

User Agent Fuzzer (1)

▶ PUT https://c0yb79yznl.execute-api.us-east-1.amazonaws.com/dev/v1/totem/order/65f255e05a8d773f94ba9fc7/status/NEW

Risk=Informativo, Confidence=Baixo (1)

https://c0yb79yznl.execute-api.us-east-1.amazonaws.com (1)

Re-examine Cache-control Directives (1)

▶ GET https://c0yb79yznl.execute-api.us-east-1.amazonaws.com/dev/v1/administrative/category

Appendix

Alert types

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

Injeção SQL

Source	raised by an active scanner (plugin ID: -1)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Injeção SQL - SQLite

Source	raised by an active scanner (plugin ID: -1)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Erro de Formato de String

Source	raised by an active scanner (Erro de Formato de String)
CWE ID	134
WASC ID	6
Reference	▪ https://owasp.org/www-community/attacks/Format_string_attack

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	▪ http://projects.webappsec.org/Cross-Site-Scripting ▪ https://cwe.mitre.org/data/definitions/79.html

Strict-Transport-Security Header Not Set

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html ▪ https://owasp.org/www-community/Security_Headers ▪ http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security ▪ http://caniuse.com/stricttransportsecurity ▪ http://tools.ietf.org/html/rfc6797

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

Re-examine Cache-control Directives

Source	raised by a passive scanner (Re-examine Cache-control Directives)
CWE ID	525
WASC ID	13
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching ▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control ▪ https://grayduck.mn/2021/09/13/cache-control-recommendations/

User Agent Fuzzer

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