ZAP Scanning Report

Generated with ZAP on qui. 8 ago. 2024, at 21:49:00

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:

- `https://octopus-app-865nn.ondigitalocean.app`
- `https://pedidos-app-zbwdu.ondigitalocean.app`
- `http://pedidos-app-zbwdu.ondigitalocean.app`

(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 (10,0%)	0 (0,0%)	0 (0,0%)	1 (10,0%)
	Baixo	0 (0,0%)	1 (10,0%)	3 (30,0%)	1 (10,0%)	5 (50,0%)
	Informativo	0 (0,0%)	0 (0,0%)	2 (20,0%)	2 (20,0%)	4 (40,0%)
	Total	0 (0,0%)	2 (20,0%)	5 (50,0%)	3 (30,0%)	10 (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://pedidos-app-zbwdu.ondigitalocean.app	0 (0)	1 (1)	2 (3)	1 (4)
	http://pedidos-app-zbwdu.ondigitalocean.app	0 (0)	0 (0)	3 (3)	3 (6)

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	2 (20,0%)
Cookie with SameSite Attribute None	Baixo	3 (30,0%)
Cookie without SameSite Attribute	Baixo	4 (40,0%)
Divulgação de Data e Hora - Unix	Baixo	8 (80,0%)
Strict-Transport-Security Header Not Set	Baixo	7 (70,0%)
X-Content-Type-Options Header Missing	Baixo	6 (60,0%)
Total		10

Alert type	Risk	Count
Cookie com Escopo Fraco	Informativo	8 (80,0%)
Re-examine Cache-control Directives	Informativo	5 (50,0%)
Session Management Response Identified	Informativo	13 (130,0%)
User Agent Fuzzer	Informativo	12 (120,0%)
Total		10

Alerts

Risk=Médio, Confidence=Alto (1)

https://pedidos-app-zbwdu.ondigitalocean.app (1)

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

▶ GET https://pedidos-app-zbwdu.ondigitalocean.app/robots.txt

Risk=Baixo, Confidence=Alto (1)

https://pedidos-app-zbwdu.ondigitalocean.app (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://pedidos-app-zbwdu.ondigitalocean.app/robots.txt

Risk=Baixo, Confidence=Médio (3)

https://pedidos-app-zbwdu.ondigitalocean.app (1)

Cookie with SameSite Attribute None (1)

▶ GET https://pedidos-app-zbwdu.ondigitalocean.app/sitemap.xml

http://pedidos-app-zbwdu.ondigitalocean.app (2)

Cookie without SameSite Attribute (1)

▶ GET http://pedidos-app-zbwdu.ondigitalocean.app/robots.txt

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

▶ GET http://pedidos-app-zbwdu.ondigitalocean.app/pedido/consulta_pedido/10

Risk=Baixo, Confidence=Baixo (1)

http://pedidos-app-zbwdu.ondigitalocean.app (1)

Divulgação de Data e Hora - Unix (1)

▶ GET http://pedidos-app-zbwdu.ondigitalocean.app/sitemap.xml

Risk=Informativo, Confidence=Médio (2)

http://pedidos-app-zbwdu.ondigitalocean.app (2)

Session Management Response Identified (1)

▶ GET http://pedidos-app-zbwdu.ondigitalocean.app/pedido/consulta_pedido/10

User Agent Fuzzer (1)

▶ GET http://pedidos-app-zbwdu.ondigitalocean.app/pedido/consulta_pedido

Risk=Informativo, Confidence=Baixo (2)

https://pedidos-app-zbwdu.ondigitalocean.app (1)

Re-examine Cache-control Directives (1)

▶ GET https://pedidos-app-zbwdu.ondigitalocean.app/pedido/consulta_pedido/10

http://pedidos-app-zbwdu.ondigitalocean.app (1)

Cookie com Escopo Fraco (1)

▶ GET http://pedidos-app-zbwdu.ondigitalocean.app/pedido/consulta_pedido/10

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 ▪ https://www.w3.org/TR/CSP/ ▪ https://w3c.github.io/webappsec-csp/ ▪ https://web.dev/articles/csp ▪ https://caniuse.com/#feat=contentsecuritypolicy ▪ https://content-security-policy.com/

Cookie with SameSite Attribute None

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Cookie without SameSite Attribute

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13

Reference	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Divulgação de Data e Hora - Unix

Source	raised by a passive scanner (Divulgação de Data e Hora)
CWE ID	200
WASC ID	13
Reference	▪ https://cwe.mitre.org/data/definitions/200.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 ▪ https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security ▪ https://caniuse.com/stricttransportsecurity ▪ https://datatracker.ietf.org/doc/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	▪ 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

Cookie com Escopo Fraco

Source	raised by a passive scanner (Cookie com Escopo Fraco)
CWE ID	565
WASC ID	15
Reference	▪ https://tools.ietf.org/html/rfc6265#section-4.1 ▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html ▪ https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

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/

Session Management Response Identified

Source	raised by a passive scanner (Session Management Response Identified)
Reference	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id

User Agent Fuzzer

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