ZAP by Checkmarx Scanning Report

Generated with ZAP on Wed 1 Oct 2025, at 05:52:29

ZAP Version: 2.16.1

ZAP by Checkmarx

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://cdnjs.cloudflare.com
- https://www.google.com
- https://accounts.google.com
- https://juice-shop.herokuapp.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: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

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	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (6.2%)	1 (6.2%)
	Medium	0 (0.0%)	2 (12.5%)	3 (18.8%)	0 (0.0%)	5 (31.2%)
	Low	0 (0.0%)	1 (6.2%)	3 (18.8%)	1 (6.2%)	5 (31.2%)
	Informational	0 (0.0%)	0 (0.0%)	3 (18.8%)	2 (12.5%)	5 (31.2%)
	Total	0 (0.0%)	3 (18.8%)	9 (56.2%)	4 (25.0%)	16 (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			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://cdnjs.cloudflare.com	0 (0)	1 (1)	0 (1)	1 (2)
	https://juice-shop.herokuapp.com	1 (1)	4 (5)	5 (10)	4 (14)

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
SQL Injection	High	1 (6.2%)
Content Security Policy (CSP) Header Not Set	Medium	95 (593.8%)
Cross-Domain Misconfiguration	Medium	100 (625.0%)
Total		16

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	36 (225.0%)
Session ID in URL Rewrite	Medium	138 (862.5%)
Vulnerable JS Library	Medium	1 (6.2%)
Cross-Domain JavaScript Source File Inclusion	Low	98 (612.5%)
Private IP Disclosure	Low	1 (6.2%)
Strict-Transport-Security Header Not Set	Low	271 (1,693.8%)
Timestamp Disclosure - Unix	Low	1098 (6,862.5%)
X-Content-Type-Options Header Missing	Low	139 (868.8%)
Information Disclosure - Suspicious Comments	Informational	4 (25.0%)
Modern Web Application	Informational	50 (312.5%)
Re-examine Cache-control Directives	Informational	130 (812.5%)
Retrieved from Cache	Informational	36 (225.0%)
User Agent Fuzzer	Informational	120 (750.0%)
Total		16

Alerts

Risk=High, Confidence=Low (1)

https://juice-shop.herokuapp.com (1)

SQL Injection (1)

▶ GET https://juice-shop.herokuapp.com/rest/products/search?q=%27%28

Risk=Medium, Confidence=High (2)

https://juice-shop.herokuapp.com (2)

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

▶ GET https://juice-shop.herokuapp.com

Session ID in URL Rewrite (1)

▶ GET https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=websocket&sid=uXLUVBBIhcv6Q9MCAAEB

Risk=Medium, Confidence=Medium (3)

https://cdnjs.cloudflare.com (1)

Vulnerable JS Library (1)

▶ GET https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js

https://juice-shop.herokuapp.com (2)

Cross-Domain Misconfiguration (1)

▶ GET https://juice-shop.herokuapp.com/assets/public/favicon_js.ico

Missing Anti-clickjacking Header (1)

▶ POST https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=PcT5DER&sid=uXLUVBBIhcv6Q9MCAAEB

Risk=Low, Confidence=High (1)

https://juice-shop.herokuapp.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://juice-shop.herokuapp.com/assets/public/favicon_js.ico

Risk=Low, Confidence=Medium (3)

https://juice-shop.herokuapp.com (3)

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://juice-shop.herokuapp.com

Private IP Disclosure (1)

▶ GET https://juice-shop.herokuapp.com/rest/admin/application-configuration

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

▶ GET https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=PcT5D9Z

Risk=Low, Confidence=Low (1)

https://juice-shop.herokuapp.com (1)

Timestamp Disclosure - Unix (1)

▶ GET https://juice-shop.herokuapp.com/assets/public/favicon_js.ico

Risk=Informational, Confidence=Medium (3)

https://cdnjs.cloudflare.com (1)

Retrieved from Cache (1)

▶ GET https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css

https://juice-shop.herokuapp.com (2)

Modern Web Application (1)

▶ GET https://juice-shop.herokuapp.com

User Agent Fuzzer (1)

▶ POST https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=PcT5Dvb&sid=uXLUVBBIhcv6Q9MCAAEB

Risk=Informational, Confidence=Low (2)

https://juice-shop.herokuapp.com (2)

Information Disclosure - Suspicious Comments (1)

▶ GET https://juice-shop.herokuapp.com/main.js

Re-examine Cache-control Directives (1)

▶ GET https://juice-shop.herokuapp.com/robots.txt

Appendix

Alert Types

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

SQL Injection

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

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/HTTP/Guides/CSP ▪ 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/

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264
WASC ID	14
Reference	▪ https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021

WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options

Session ID in URL Rewrite

Source	raised by a passive scanner (Session ID in URL Rewrite)
CWE ID	598
WASC ID	13
Reference	▪ https://seclists.org/webappsec/2002/q4/111

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	1395
Reference	▪ https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

Private IP Disclosure

Source	raised by a passive scanner (Private IP Disclosure)
CWE ID	497
WASC ID	13
Reference	▪ https://datatracker.ietf.org/doc/html/rfc1918

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

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)

CWE ID	497
WASC ID	13
Reference	▪ https://cwe.mitre.org/data/definitions/200.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

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	615
WASC ID	13

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

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/Reference/Headers/Cache-Control ▪ https://grayduck.mn/2021/09/13/cache-control-recommendations/

Retrieved from Cache

Source	raised by a passive scanner (Retrieved from Cache)
CWE ID	525
Reference	▪ https://datatracker.ietf.org/doc/html/rfc7234 ▪ https://datatracker.ietf.org/doc/html/rfc7231 ▪ https://www.rfc-editor.org/rfc/rfc9110.html

User Agent Fuzzer

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