

ZAP by Checkmarx

Scanning Report

Generated with  ZAP on Wed 13 Aug 2025, at 17:24:01

ZAP Version: 2.16.0

ZAP by Checkmarx

Contents

- [About this report](#)
 - [Report parameters](#)
- [Summaries](#)
 - [Alert counts by risk and confidence](#)
 - [Alert counts by site and risk](#)
 - [Alert counts by alert type](#)
- [Alerts](#)
 - [Risk=Medium, Confidence=High \(2\)](#)
 - [Risk=Medium, Confidence=Medium \(3\)](#)
 - [Risk=Medium, Confidence=Low \(1\)](#)
 - [Risk=Low, Confidence=Medium \(3\)](#)

- [Risk=Low, Confidence=Low \(1\)](#).
- [Risk=Informational, Confidence=Medium \(2\)](#).
- [Risk=Informational, Confidence=Low \(1\)](#).
- [Appendix](#)
 - [Alert types](#)

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- <http://cdnjs.cloudflare.com>
- <http://localhost:3000>

(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				
Risk		User Confirmed	High	Medium	Low	Total
	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	2 (15.4%)	3 (23.1%)	1 (7.7%)	6 (46.2%)
	Low	0 (0.0%)	0 (0.0%)	3 (23.1%)	1 (7.7%)	4 (30.8%)
	Informational	0 (0.0%)	0 (0.0%)	2 (15.4%)	1 (7.7%)	3 (23.1%)
	1					
Total		0 (0.0%)	2 (15.4%)	8 (61.5%)	3 (23.1%)	13 (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.)

Site	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
http://cdnjs.cloudflare.com	0 (0)	1 (1)	0 (1)	1 (2)
http://localhost:3000	0 (0)	5 (5)	4 (9)	2 (11)

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	Medium	18 (138.5%)
Cross-Domain Misconfiguration	Medium	51 (392.3%)
Total		13

Alert type	Risk	Count
Hidden File Found	Medium	4 (30.8%)
Missing Anti-clickjacking Header	Medium	6 (46.2%)
Session ID in URL Rewrite	Medium	27 (207.7%)
Vulnerable JS Library	Medium	1 (7.7%)
Cross-Domain JavaScript Source File Inclusion	Low	4 (30.8%)
Private IP Disclosure	Low	1 (7.7%)
Timestamp Disclosure - Unix	Low	21 (161.5%)
X-Content-Type-Options Header Missing	Low	27 (207.7%)
Information Disclosure - Suspicious Comments	Informational	4 (30.8%)
Modern Web Application	Informational	3 (23.1%)
Retrieved from Cache	Informational	9 (69.2%)
Total		13

Alerts

Risk=Medium, Confidence=High (2)

<http://localhost:3000> (2)

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

► GET <http://localhost:3000/sitemap.xml>

Session ID in URL Rewrite (1)

► POST <http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PYZNVnp&sid=itvE-VwXdav6bu7AAAAQ>

Risk=Medium, Confidence=Medium (3)

<http://cdnjs.cloudflare.com> (1)

Vulnerable JS Library (1)

► GET
<http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js>

<http://localhost:3000> (2)

Cross-Domain Misconfiguration (1)

► GET <http://localhost:3000/robots.txt>

Missing Anti-clickjacking Header (1)

► POST <http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PYZNVnp&sid=itvE-VwXdav6bu7AAAAQ>

Risk=Medium, Confidence=Low (1)

http://localhost:3000 (1)

Hidden File Found (1)

► GET http://localhost:3000/.hg

Risk=Low, Confidence=Medium (3)

http://localhost:3000 (3)

Cross-Domain JavaScript Source File Inclusion (1)

► GET http://localhost:3000/sitemap.xml

Private IP Disclosure (1)

► GET http://localhost:3000/rest/admin/application-configuration

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

► GET http://localhost:3000/socket.io/?
EIO=4&transport=polling&t=PYZNVZh

Risk=Low, Confidence=Low (1)

http://localhost:3000 (1)

Timestamp Disclosure - Unix (1)

► GET http://localhost:3000/

Risk=Informational, Confidence=Medium (2)

<http://cdnjs.cloudflare.com> (1)

Retrieved from Cache (1)

► GET

<http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css>

<http://localhost:3000> (1)

Modern Web Application (1)

► GET <http://localhost:3000/sitemap.xml>

Risk=Informational, Confidence=Low (1)

<http://localhost:3000> (1)

Information Disclosure - Suspicious Comments (1)

► GET <http://localhost:3000/main.js>

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	<ul style="list-style-type: none">▪ 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/

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264
WASC ID	14
Reference	<ul style="list-style-type: none">▪ https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_c

Hidden File Found

Source	raised by an active scanner (Hidden File Finder)
CWE ID	538
WASC ID	13
Reference	<ul style="list-style-type: none">▪ https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	<ul style="list-style-type: none">▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Session ID in URL Rewrite

Source	raised by a passive scanner (Session ID in URL Rewrite)
CWE ID	200
WASC ID	13
Reference	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ https://github.com/jquery/jquery/issues/2432▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/▪ http://research.insecurelabs.org/jquery/test/▪ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/▪ https://nvd.nist.gov/vuln/detail/CVE-2019-11358▪ https://github.com/advisories/GHSA-rmxg-73gg-4p98▪ https://nvd.nist.gov/vuln/detail/CVE-2015-9251▪ https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b▪ https://github.com/jquery/jquery.com/issues/162▪ https://bugs.jquery.com/ticket/11974▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

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 [200](#)

WASC ID 13

Reference

- <https://tools.ietf.org/html/rfc1918>

Timestamp Disclosure - Unix

Source raised by a passive scanner ([Timestamp Disclosure](#))

CWE ID [200](#)

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://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 [200](#)

WASC ID 13

Modern Web Application

Source raised by a passive scanner ([Modern Web Application](#))

Retrieved from Cache

Source raised by a passive scanner ([Retrieved from Cache](#))

- Reference**
- <https://tools.ietf.org/html/rfc7234>
 - <https://tools.ietf.org/html/rfc7231>
 - <https://www.rfc-editor.org/rfc/rfc9110.html>

