

Linkedin-Clone-Scan-Report

Generated with  ZAP on Sat 19 Nov 2022, at 18:49:48

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=Low, Confidence=High \(1\)](#)
 - [Risk=Low, Confidence=Medium \(2\)](#)
 - [Risk=Low, Confidence=Low \(1\)](#)
 - [Risk=Informational, Confidence=Medium \(3\)](#)

- [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://localhost:8100>
- <https://www.google.com>
- <http://ocsp.pki.goog>
- <http://ocsp.digicert.com>
- <http://r3.o.lencr.org>

(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%)	0 (0.0%)	5 (38.5%)
	Low	0 (0.0%)	1 (7.7%)	2 (15.4%)	1 (7.7%)	4 (30.8%)
	Informational	0 (0.0%)	0 (0.0%)	3 (23.1%)	1 (7.7%)	4 (30.8%)
	1	0 (0.0%)	0 (0.0%)	3 (23.1%)	1 (7.7%)	4 (30.8%)
Total		0 (0.0%)	3 (23.1%)	8 (61.5%)	2 (15.4%)	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				Informational
	High (= High)	Medium (>= Medium)	Low (>= Low)	(>= Informational)	
http://localhost:8100	0 (0)	4 (4)	2 (6)	3 (9)	
http://ocsp.pki.goog	0 (0)	1 (1)	0 (1)	0 (1)	
http://ocsp.digicert.com	0 (0)	0 (0)	2 (2)	1 (3)	

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
Application Error Disclosure	Medium	1 (7.7%)
Total		13

Alert type	Risk	Count
CSP: Wildcard Directive	Medium	5 (38.5%)
Content Security Policy (CSP) Header Not Set	Medium	3 (23.1%)
Cross-Domain Misconfiguration	Medium	32 (246.2%)
Missing Anti-clickjacking Header	Medium	2 (15.4%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	28 (215.4%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1 (7.7%)
Timestamp Disclosure - Unix	Low	1 (7.7%)
X-Content-Type-Options Header Missing	Low	31 (238.5%)
Content-Type Header Missing	Informational	2 (15.4%)
Information Disclosure - Suspicious Comments	Informational	9 (69.2%)
Modern Web Application	Informational	5 (38.5%)
Retrieved from Cache	Informational	1 (7.7%)
Total		13

Alerts

Risk=Medium, Confidence=High (2)

<http://localhost:8100> (1)

CSP: Wildcard Directive (1)

► GET <http://localhost:8100/robots.txt>

<http://ocsp.pki.goog> (1)

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

► GET <http://ocsp.pki.goog/gts1c3>

Risk=Medium, Confidence=Medium (3)

<http://localhost:8100> (3)

Application Error Disclosure (1)

► GET <http://localhost:8100/8991.js>

Cross-Domain Misconfiguration (1)

► GET <http://localhost:8100/runtime.js>

Missing Anti-clickjacking Header (1)

► GET <http://localhost:8100/>

Risk=Low, Confidence=High (1)

<http://ocsp.digicert.com> (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

► GET <http://ocsp.digicert.com/>

Risk=Low, Confidence=Medium (2)

<http://localhost:8100> (1)

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

► GET <http://localhost:8100/runtime.js>

<http://ocsp.digicert.com> (1)

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

► GET <http://ocsp.digicert.com/>

Risk=Low, Confidence=Low (1)

<http://localhost:8100> (1)

Timestamp Disclosure - Unix (1)

► GET <http://localhost:8100/sockjs-node/info?t=1668865472878>

Risk=Informational, Confidence=Medium (3)

<http://localhost:8100> (2)

Content-Type Header Missing (1)

► GET <http://localhost:8100/sockjs-node/058/ct42wqrc/websocket>

Modern Web Application (1)

► GET <http://localhost:8100/>

<http://ocsp.digicert.com> (1)

Retrieved from Cache (1)

► GET <http://ocsp.digicert.com/>

Risk=Informational, Confidence=Low (1)

<http://localhost:8100> (1)

Information Disclosure - Suspicious Comments (1)

► GET <http://localhost:8100/styles.js>

Appendix

Alert types

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

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none">▪ http://www.w3.org/TR/CSP2/▪ http://www.w3.org/TR/CSP/▪ http://caniuse.com/#search=content+security+policy▪ http://content-security-policy.com/▪ https://github.com/shapesecurity/salvation▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

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▪ http://www.w3.org/TR/CSP/▪ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html▪ http://www.html5rocks.com/en/tutorials/security/content-security-policy/▪ http://caniuse.com/#feat=contentsecuritypolicy▪ http://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?id=desc.config.dotnet.html5_overly_permissive_cors_policy

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

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
CWE ID	200
WASC ID	13
Reference	<ul style="list-style-type: none">▪ http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx▪ http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200

WASC ID 13

Reference

- <http://httpd.apache.org/docs/current/mod/core.html#servertokens>
- http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
- <http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx>
- <http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html>

Timestamp Disclosure - Unix

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

CWE ID [200](#)

WASC ID 13

Reference

- <http://projects.webappsec.org/w/page/13246936/Information%20Leakage>

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>

Content-Type Header Missing

Source raised by a passive scanner ([Content-Type Header Missing](#))

CWE ID [345](#)

WASC ID 12

Reference ▪ <http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx>

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>
- <http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html> (obsoleted by rfc7234).