

StaggingN2N ZAP

Scanning Report

Generated with  ZAP on Mon 19 Dec 2022, at 09:38:39

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

- [Risk=Informational, Confidence=Medium \(2\)](#)
- [Risk=Informational, Confidence=Low \(2\)](#)
- [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:

- <https://staggingn2n.web.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: [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%)	1 (8.3%)	0 (0.0%)	0 (0.0%)	1 (8.3%)
	Medium	0 (0.0%)	1 (8.3%)	1 (8.3%)	0 (0.0%)	2 (16.7%)
	Low	0 (0.0%)	1 (8.3%)	3 (25.0%)	1 (8.3%)	5 (41.7%)
	Informational	0 (0.0%)	0 (0.0%)	2 (16.7%)	2 (16.7%)	4 (33.3%)
	1	0 (0.0%)	0 (0.0%)	2 (16.7%)	2 (16.7%)	4 (33.3%)
Total		0 (0.0%)	3 (25.0%)	6 (50.0%)	3 (25.0%)	12 (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)
https://staggingn2n.web.app	1 (1)	2 (3)	5 (8)	4 (12)

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
PII Disclosure	High	3 (25.0%)
Content Security Policy (CSP) Header Not Set	Medium	4 (33.3%)
Missing Anti-clickjacking Header	Medium	4 (33.3%)
Cross-Domain JavaScript Source File Inclusion	Low	4 (33.3%)
Total		12

Alert type	Risk	Count
Private IP Disclosure	Low	1 (8.3%)
Strict-Transport-Security Header Not Set	Low	1 (8.3%)
Timestamp Disclosure - Unix	Low	3 (25.0%)
X-Content-Type-Options Header Missing	Low	15 (125.0%)
Information Disclosure - Suspicious Comments	Informational	4 (33.3%)
Modern Web Application	Informational	5 (41.7%)
Re-examine Cache-control Directives	Informational	5 (41.7%)
Retrieved from Cache	Informational	6 (50.0%)
Total		12

Alerts

Risk=High, Confidence=High (1)

<https://staggingn2n.web.app> (1)

PII Disclosure (1)

► GET

<https://staggingn2n.web.app/main.c7440cbe4ea538d3adb6.chunk.js>

Risk=Medium, Confidence=High (1)

<https://staggingn2n.web.app> (1)

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

► GET <https://staggingn2n.web.app/>

Risk=Medium, Confidence=Medium (1)

<https://staggingn2n.web.app> (1)

Missing Anti-clickjacking Header (1)

► GET <https://staggingn2n.web.app/>

Risk=Low, Confidence=High (1)

<https://staggingn2n.web.app> (1)

Strict-Transport-Security Header Not Set (1)

► GET

<https://staggingn2n.web.app/vendor.b2abe1a857609739682f.chunk.js>

Risk=Low, Confidence=Medium (3)

<https://staggingn2n.web.app> (3)

Cross-Domain JavaScript Source File Inclusion (1)

► GET https://staggingn2n.web.app/

Private IP Disclosure (1)

► GET

https://staggingn2n.web.app/vendor.b2abe1a857609739682f.chunk.js

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

► GET https://staggingn2n.web.app/

Risk=Low, Confidence=Low (1)

https://staggingn2n.web.app (1)

Timestamp Disclosure - Unix (1)

► GET

https://staggingn2n.web.app/vendor.b2abe1a857609739682f.chunk.js

Risk=Informational, Confidence=Medium (2)

https://staggingn2n.web.app (2)

Modern Web Application (1)

► GET https://staggingn2n.web.app/

Retrieved from Cache (1)

► GET https://staggingn2n.web.app

Risk=Informational, Confidence=Low (2)

<https://staggingn2n.web.app> (2)

Information Disclosure - Suspicious Comments (1)

► GET

<https://staggingn2n.web.app/main.c7440cbe4ea538d3adb6.chunk.js>

Re-examine Cache-control Directives (1)

► GET <https://staggingn2n.web.app/>

Appendix

Alert types

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

PII Disclosure

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

CWE ID [359](#)

WASC ID 13

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
- <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/>

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/Headers/X-Frame-Options

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	<ul style="list-style-type: none">▪ https://tools.ietf.org/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	<ul style="list-style-type: none">▪ 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_Transpo

rt Security

- <http://caniuse.com/stricttransportsecurity>
- <http://tools.ietf.org/html/rfc6797>

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13
Reference	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx▪ 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)
---------------	--

Re-examine Cache-control Directives

Source	raised by a passive scanner (Re-examine Cache-control Directives)
CWE ID	525
WASC ID	13
Reference	<ul style="list-style-type: none">▪ 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/

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).