Staff Genix TLC Scanning Report

Generated with ZAP on Mon 30 Jan 2023, at 15:29:30

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://staggingtlc.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				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	1 (9.1%)	0 (0.0%)	0 (0.0%)	1 (9.1%)
	Medium	0 (0.0%)	1 (9.1%)	1 (9.1%)	0 (0.0%)	2 (18.2%)
	Low	0 (0.0%)	0 (0.0%)	3 (27.3%)	1 (9.1%)	4 (36.4%)
	Informational	0 (0.0%)	0 (0.0%)	2 (18.2%)	2 (18.2%)	4 (36.4%)
	Total	0 (0.0%)	2 (18.2%)	6 (54.5%)	3 (27.3%)	11 (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://staggingtlc.web.app	1 (1)	2 (3)	4 (7)	4 (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
PII Disclosure	High	3 (27.3%)
Content Security Policy (CSP) Header Not Set	Medium	5 (45.5%)
Missing Anti-clickjacking Header	Medium	5 (45.5%)
Cross-Domain JavaScript Source File Inclusion	Low	5 (45.5%)
Private IP Disclosure	Low	1 (9.1%)
Total		11

Alert type	Risk	Count
Timestamp Disclosure - Unix	Low	3 (27.3%)
X-Content-Type-Options Header Missing	Low	29 (263.6%)
Information Disclosure - Suspicious Comments	Informational	8 (72.7%)
Modern Web Application	Informational	6 (54.5%)
Re-examine Cache-control Directives	Informational	5 (45.5%)
Retrieved from Cache	Informational	7 (63.6%)
Total		11

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

▶ GET
https://staggingtlc.web.app/main.0cb78aa72fda0c7b71d8.chunk.js

Risk=Medium, Confidence=High (1)

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

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

▶ GET https://staggingtlc.web.app/

Risk=Medium, Confidence=Medium (1)

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

Missing Anti-clickjacking Header (1)

▶ GET https://staggingtlc.web.app/

Risk=Low, Confidence=Medium (3)

https://staggingtlc.web.app (3)

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://staggingtlc.web.app/

Private IP Disclosure (1)

▶ GET
https://staggingtlc.web.app/vendor.2be8802a19443eeb2862.chunk.js

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

▶ GET https://staggingtlc.web.app

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET
https://staggingtlc.web.app/vendor.2be8802a19443eeb2862.chunk.js

Risk=Informational, Confidence=Medium (2)

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

Modern Web Application (1)

▶ GET https://staggingtlc.web.app/

Retrieved from Cache (1)

▶ GET https://staggingtlc.web.app

Risk=Informational, Confidence=Low (2)

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

Information Disclosure - Suspicious Comments (1)

▶ GET
https://staggingtlc.web.app/main.0cb78aa72fda0c7b71d8.chunk.js

Re-examine Cache-control Directives (1)

▶ GET https://staggingtlc.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	▪ https://tools.ietf.org/html/rfc1918

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

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	▪ 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)