

Staff Genix-BrandAdmin- NoFPRemoved (InThesis)-11-4-23

Generated with  ZAP on Tue 11 Apr 2023, at 16:29:30

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 \(2\)](#)
 - [Risk=Low, Confidence=Medium \(1\)](#)
 - [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://stagingbrandadmin.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 (11.1%)	0 (0.0%)	0 (0.0%)	1 (11.1%)
	Medium	0 (0.0%)	2 (22.2%)	0 (0.0%)	0 (0.0%)	2 (22.2%)
	Low	0 (0.0%)	0 (0.0%)	1 (11.1%)	1 (11.1%)	2 (22.2%)
	Informational	0 (0.0%)	0 (0.0%)	2 (22.2%)	2 (22.2%)	4 (44.4%)
	1					
Total		0 (0.0%)	3 (33.3%)	3 (33.3%)	3 (33.3%)	9 (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			Informational
		High (= High)	Medium (>= Medium)	Low (>= Low)	
Site	https://stagingbrand.admin.web.app	1 (1)	2 (3)	2 (5)	4 (9)

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 (33.3%)
CSP: script-src unsafe-eval	Medium	5 (55.6%)
CSP: style-src unsafe-inline	Medium	5 (55.6%)
Private IP Disclosure	Low	1 (11.1%)
Total		9

Alert type	Risk	Count
Timestamp Disclosure - Unix	Low	77 (855.6%)
Information Disclosure - Suspicious Comments	Informational	7 (77.8%)
Modern Web Application	Informational	5 (55.6%)
Re-examine Cache-control Directives	Informational	5 (55.6%)
Retrieved from Cache	Informational	9 (100.0%)
Total		9

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

► GET

https://stagingbrandadmin.web.app/main.f7f553f1047bbd984b88.chunk.js

Risk=Medium, Confidence=High (2)

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

CSP: script-src unsafe-eval (1)

► GET <https://stagingbrandadmin.web.app/>

CSP: style-src unsafe-inline (1)

► GET <https://stagingbrandadmin.web.app/>

Risk=Low, Confidence=Medium (1)

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

Private IP Disclosure (1)

► GET

<https://stagingbrandadmin.web.app/vendor.35e89c0b8b7b492e2c32.chunk.js>

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

► GET

<https://stagingbrandadmin.web.app/vendor.35e89c0b8b7b492e2c32.chunk.js>

Risk=Informational, Confidence=Medium (2)

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

Modern Web Application (1)

► GET <https://stagingbrandadmin.web.app/>

Retrieved from Cache (1)

► GET <https://stagingbrandadmin.web.app>

Risk=Informational, Confidence=Low (2)

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

Information Disclosure - Suspicious Comments (1)

► GET
<https://stagingbrandadmin.web.app/main.f7f553f1047bbd984b88.chunk.js>

Re-examine Cache-control Directives (1)

► GET <https://stagingbrandadmin.web.app/sitemap.xml>

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

CSP: script-src unsafe-eval

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

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693

WASC ID

15

Reference

- <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

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>

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).