StaffGenix Brand Admin Report

Generated with ZAP on Fri 4 Nov 2022, at 12:08:45

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://unpkg.com
- https://cdnjs.cloudflare.com
- https://fonts.googleapis.com
- https://stagingbrandadmin.web.app
- https://web.whatsapp.com
- https://googleads.g.doubleclick.net
- https://adservice.google.com.pk
- https://adservice.google.com
- https://play.google.com
- https://apis.google.com
- https://www.google.com

(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 (4.2%)	0 (0.0%)	0 (0.0%)	1 (4.2%)
	Medium	0 (0.0%)	4 (16.7%)	4 (16.7%)	1 (4.2%)	9 (37.5%)
	Low	0 (0.0%)	2 (8.3%)	4 (16.7%)	1 (4.2%)	7 (29.2%)

	Confidence				
	User Confirmed	High	Medium	Low	Total
Informational	0 (0.0%)	0 (0.0%)	3 (12.5%)	4 (16.7%)	7 (29.2%)
Total	0 (0.0%)	7 (29.2%)	11 (45.8%)	6 (25.0%)	24 (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://cdnjs.cloudflare.com	0 (0)	1 (1)	0 (1)	0 (1)
	https://fonts.googleapis.com	0 (0)	1 (1)	0 (1)	0 (1)
	https://stagingbrandadmin.web.app	1 (1)	1 (2)	1 (3)	0 (3)
	https://web.whatsapp.com	0 (0)	2 (2)	0 (2)	0 (2)

	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://apis.google.com	0 (0)	0 (0)	1 (1)	2 (3)
https://www.google.com	0 (0)	4 (4)	5 (9)	5 (14)

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	1 (4.2%)
Absence of Anti-CSRF Tokens	Medium	1 (4.2%)
Application Error Disclosure	Medium	3 (12.5%)
CSP: Wildcard Directive	Medium	5 (20.8%)
CSP: script-src unsafe-inline	Medium	3
Total		24

Alert type	Risk	Count
		(12.5%)
CSP: style-src unsafe-inline	Medium	5 (20.8%)
Content Security Policy (CSP) Header Not Set	Medium	22 (91.7%)
Cross-Domain Misconfiguration	Medium	6 (25.0%)
Missing Anti-clickjacking Header	Medium	1 (4.2%)
Vulnerable JS Library	Medium	1 (4.2%)
CSP: Notices	Low	2 (8.3%)
Cookie No HttpOnly Flag	Low	4 (16.7%)
Cookie with SameSite Attribute None	Low	4 (16.7%)
Cross-Domain JavaScript Source File Inclusion	Low	3 (12.5%)
Strict-Transport-Security Header Not Set	Low	35 (145.8%)
Timestamp Disclosure - Unix	Low	135 (562.5%)
Total		24

Alert type	Risk	Count
X-Content-Type-Options Header Missing	Low	6 (25.0%)
Information Disclosure - Sensitive Information in URL	Informational	9 (37.5%)
Information Disclosure - Suspicious Comments	Informational	33 (137.5%)
Loosely Scoped Cookie	Informational	4 (16.7%)
Modern Web Application	Informational	6 (25.0%)
Re-examine Cache-control Directives	Informational	10 (41.7%)
Retrieved from Cache	Informational	4 (16.7%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	3 (12.5%)
Total		24

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

▶ GET https://stagingbrandadmin.web.app/main.0b7bb8c332e38a8a8144.chunk.js

Risk=Medium, Confidence=High (4)

https://web.whatsapp.com (1)

CSP: script-src unsafe-inline (1)

▶ GET https://web.whatsapp.com/

https://www.google.com (3)

CSP: Wildcard Directive (1)

▶ GET https://www.google.com/search?client=firefox-b-d&q=adobe+reader

CSP: style-src unsafe-inline (1)

▶ GET https://www.google.com/search?client=firefox-b-d&q=adobe+reader

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

▶ POST https://www.google.com/gen_204?atyp=i&ei=GltlY_uqJLuJ9u8Pk4iKyAI&ct=slh&v=t1&im=M&pv=0.4273714466292179&me=230:1667587129985,V,0,0,0,0:24357,V,0,1080,1280,595:558,e,H&zx=1667587154901

Risk=Medium, Confidence=Medium (4)

https://cdnjs.cloudflare.com (1)

Vulnerable JS Library (1)

▶ GET https://cdnjs.cloudflare.com/ajax/libs/moment.js/2.18.1/moment.min.js

https://fonts.googleapis.com (1)

Cross-Domain Misconfiguration (1)

▶ GET https://fonts.googleapis.com/css?family=Open+Sans:400,600,700

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

Missing Anti-clickjacking Header (1)

▶ GET https://stagingbrandadmin.web.app/

https://web.whatsapp.com (1)

Application Error Disclosure (1)

▶ GET https://web.whatsapp.com/

Risk=Medium, Confidence=Low (1)

https://www.google.com (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.google.com/search?client=firefox-b-d&q=adobe+reader

Risk=Low, Confidence=High (2)

https://www.google.com (2)

CSP: Notices (1)

▶ GET https://www.google.com/search?client=firefox-b-d&q=adobe+reader

Strict-Transport-Security Header Not Set (1)

▶ POST https://www.google.com/gen_204?atyp=i&ei=GltlY_uqJLuJ9u8Pk4iKyAI&ct=slh&v=t1&im=M&pv=0.4273714466292179&me=230:1667587129985,V,0,0,0,0:24357,V,0,1080,1280,595:558,e,H&zx=1667587154901

Risk=Low, Confidence=Medium (4)

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

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://stagingbrandadmin.web.app/

https://www.google.com (3)

Cookie No HttpOnly Flag (1)

▶ GET https://www.google.com/search?client=firefox-b-d&q=adobe+reader

Cookie with SameSite Attribute None (1)

▶ GET https://www.google.com/search?client=firefox-b-d&q=adobe+reader

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

▶ GET https://www.google.com/compressiontest/gzip.html

Risk=Low, Confidence=Low (1)

https://apis.google.com (1)

Timestamp Disclosure - Unix (1)

▶ GET https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.7I3T5S8x4Qg.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo9SzNpm6HglASFo9cZ-GgP5E5f5WQ/cb=gapi.loaded_0

Risk=Informational, Confidence=Medium (3)

https://apis.google.com (1)

Retrieved from Cache (1)

▶ GET https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.7I3T5S8x4Qg.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo9SzNpm6HglASFo9cZ-GgP5E5f5WQ/cb=gapi.loaded_0

https://www.google.com (2)

Information Disclosure - Sensitive Information in URL (1)

▶ POST https://www.google.com/gen_204?atyp=i&ei=GltlY_uqJLuJ9u8Pk4iKyAI&ct=slh&v=t1&im=M&pv=0.427371446 6292179&me=230:1667587129985,V,0,0,0,0:24357,V,0,1080,1280,595:55 8,e,H&zx=1667587154901

Modern Web Application (1)

▶ GET https://www.google.com/compressiontest/gzip.html

Risk=Informational, Confidence=Low (4)

https://apis.google.com (1)

Information Disclosure - Suspicious Comments (1)

▶ GET https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.7I3T5S8x4Qg.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo9SzNpm6HglASFo9cZ-GgP5E5f5WQ/cb=gapi.loaded_0

https://www.google.com (3)

Loosely Scoped Cookie (1)

▶ GET https://www.google.com/search?client=firefox-b-d&q=adobe+reader

Re-examine Cache-control Directives (1)

▶ GET https://www.google.com/search?client=firefox-b-d&q=adobe+reader

User Controllable HTML Element Attribute (Potential XSS) (1)

▶ GET https://www.google.com/search?client=firefox-b-d&q=adobe+reader

Appendix

Alert types

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

PII Disclosure

Source	raised by a passive scanner (plugin ID: -1)
CWE ID	359
WASC ID	13

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery

- http://cwe.mitre.org/data/definitions/352.html

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	• 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: script-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

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

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/

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	• https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18214

- https://github.com/moment/moment/security/advisories/GHSA-wc69-rhjr-hc9g
- https://security.snyk.io/vuln/npm:moment:20170905
- https://security.snyk.io/vuln/SNYK-JS-MOMENT-2944238
- https://github.com/moment/moment/security/advisories/GHSA-8hfj-j24r-96c4
- https://github.com/moment/moment/issues/4163

CSP: Notices

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

Cookie No HttpOnly Flag

Source	raised by a passive scanner (Cookie No HttpOnly Flag)
CWE ID	1004
WASC ID	13
Reference	- https://owasp.org/www-community/HttpOnly

Cookie with SameSite Attribute None

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	- https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

Strict-Transport-Security Header Not Set

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	▪ 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_Transport_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	▪ 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 - Sensitive Information in URL

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	200
WASC ID	13

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
WASC ID	13

Loosely Scoped Cookie

Source	raised by a passive scanner (Loosely Scoped Cookie)

CWE ID	565
WASC ID	15
Reference	▪ https://tools.ietf.org/html/rfc6265#section-4.1 ▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html ▪ http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

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)

User Controllable HTML Element Attribute (Potential XSS)

Source raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS))

CWE ID 20

WASC ID 20

Reference
- http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute