CrateShop-Scan-Report

Generated with ZAP on Mon 14 Nov 2022, at 16:02:32

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://fonts.gstatic.com
- https://fonts.googleapis.com
- http://localhost:3000

(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 (6.7%)	0 (0.0%)	0 (0.0%)	1 (6.7%)
	Medium	0 (0.0%)	2 (13.3%)	2 (13.3%)	1 (6.7%)	5 (33.3%)
	Low	0 (0.0%)	1 (6.7%)	2 (13.3%)	1 (6.7%)	4 (26.7%)
	Informational	0 (0.0%)	0 (0.0%)	4 (26.7%)	1 (6.7%)	5 (33.3%)
	Total	0 (0.0%)	4 (26.7%)	8 (53.3%)	3 (20.0%)	15 (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://fonts.gstatic.com	0 (0)	0 (0)	1 (1)	1 (2)
	https://fonts.googleapis.com	0 (0)	1 (1)	0 (1)	0 (1)
	http://localhost:3000	1 (1)	4 (5)	3 (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
Content Security Policy (CSP) Header Not Set	High	1 (6.7%)
Total		15

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	4 (26.7%)
CSP: Wildcard Directive	Medium	5 (33.3%)
Content Security Policy (CSP) Header Not Set	Medium	18 (120.0%)
Cross-Domain Misconfiguration	Medium	5 (33.3%)
Missing Anti-clickjacking Header	Medium	9 (60.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	62 (413.3%)
Strict-Transport-Security Header Not Set	Low	2 (13.3%)
Timestamp Disclosure - Unix	Low	112 (746.7%)
X-Content-Type-Options Header Missing	Low	47 (313.3%)
Information Disclosure - Sensitive Information in URL	Informational	4 (26.7%)
Information Disclosure - Suspicious Comments	Informational	112 (746.7%)
Modern Web Application	Informational	4 (26.7%)
Total		15

Alert type	Risk	Count
Retrieved from Cache	Informational	2 (13.3%)
User Agent Fuzzer	Informational	336 (2,240.0%)
Total		15

Alerts

Risk=High, Confidence=High (1)

http://localhost:3000 (1)

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

▶ GET http://localhost:3000/

Risk=Medium, Confidence=High (2)

http://localhost:3000 (2)

CSP: Wildcard Directive (1)

▶ GET http://localhost:3000/css

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

▶ GET http://localhost:3000/

Risk=Medium, Confidence=Medium (2)

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

Cross-Domain Misconfiguration (1)

▶ GET https://fonts.googleapis.com/css?family=Lobster

http://localhost:3000 (1)

Missing Anti-clickjacking Header (1)

▶ GET http://localhost:3000/

Risk=Medium, Confidence=Low (1)

http://localhost:3000 (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://localhost:3000/user/login

Risk=Low, Confidence=High (1)

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

Strict-Transport-Security Header Not Set (1)

▶ GET
https://fonts.gstatic.com/s/roboto/v30/KFOmCnqEu92Fr1Mu4mxK.woff2

Risk=Low, Confidence=Medium (2)

http://localhost:3000 (2)

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

▶ GET http://localhost:3000/css/common.css

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

▶ GET http://localhost:3000/css/common.css

Risk=Low, Confidence=Low (1)

http://localhost:3000 (1)

Timestamp Disclosure - Unix (1)

▶ GET http://localhost:3000/js/bundles/app.js?0.8815465050430795

Risk=Informational, Confidence=Medium (4)

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

Retrieved from Cache (1)

▶ GET
https://fonts.gstatic.com/s/roboto/v30/KFOmCnqEu92Fr1Mu4mxK.woff2

http://localhost:3000 (3)

Information Disclosure - Sensitive Information in URL (1)

▶ GET http://localhost:3000/user/login?email=foo-bar%40example.com&password=ZAP

Modern Web Application (1)

▶ GET http://localhost:3000/

User Agent Fuzzer (1)

▶ GET http://localhost:3000/css

Risk=Informational, Confidence=Low (1)

http://localhost:3000 (1)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost:3000/js/service-worker.js

Appendix

Alert types

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

Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (plugin ID: -1)
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/

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

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

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

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

- 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

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

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)

User Agent Fuzzer

Source	raised by an active scanner (User Agent Fuzzer)
Reference	▪ https://owasp.org/wstg