RabitaBankClone-Scan-Report

Generated with ZAP on Tue 15 Nov 2022, at 23:20:38

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%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	2 (20.0%)	2 (20.0%)	0 (0.0%)	4 (40.0%)
	Low	0 (0.0%)	1 (10.0%)	2 (20.0%)	0 (0.0%)	3 (30.0%)
	Informational	0 (0.0%)	0 (0.0%)	3 (30.0%)	0 (0.0%)	3 (30.0%)
	Total	0 (0.0%)	3 (30.0%)	7 (70.0%)	0 (0.0%)	10 (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)
	http://localhost:3000	0 (0)	4 (4)	2 (6)	2 (8)

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
CSP: Wildcard Directive	Medium	8 (80.0%)
Content Security Policy (CSP) Header Not Set	Medium	4 (40.0%)
Cross-Domain Misconfiguration	Medium	23 (230.0%)
Missing Anti-clickjacking Header	Medium	4 (40.0%)
Total		10

Alert type	Risk	Count
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	17 (170.0%)
Strict-Transport-Security Header Not Set	Low	5 (50.0%)
X-Content-Type-Options Header Missing	Low	11 (110.0%)
Information Disclosure - Suspicious Comments	Informational	19 (190.0%)
Modern Web Application	Informational	5 (50.0%)
Retrieved from Cache	Informational	5 (50.0%)
Total		10

Alerts

Risk=Medium, Confidence=High (2)

http://localhost:3000 (2)

CSP: Wildcard Directive (1)

▶ GET http://localhost:3000/sitemap.xml

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

▶ GET http://localhost:3000/

Risk=Medium, Confidence=Medium (2)

http://localhost:3000 (2)

Cross-Domain Misconfiguration (1)

▶ GET http://localhost:3000/

Missing Anti-clickjacking Header (1)

▶ GET http://localhost:3000/

Risk=Low, Confidence=High (1)

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

Strict-Transport-Security Header Not Set (1)

▶ GET https://fonts.gstatic.com/s/notosansjp/v42/-F62fjtqLzI2JPCgQBnw7HFow2oe2EcP5pp0erwTqsSWs9Jezazjcb4.117.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/

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

▶ GET http://localhost:3000/

Risk=Informational, Confidence=Medium (3)

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

Retrieved from Cache (1)

▶ GET https://fonts.gstatic.com/s/notosansjp/v42/-F62fjtqLzI2JPCgQBnw7HFow2oe2EcP5pp0erwTqsSWs9Jezazjcb4.117.woff2

http://localhost:3000 (2)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost:3000/

Modern Web Application (1)

▶ GET http://localhost:3000/

Appendix

Alert types

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

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

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)

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)