Amazon-Clone-2-Scan-Report

Generated with ZAP on Fri 18 Nov 2022, at 21:20:16

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://m.stripe.com
- https://m.stripe.network
- https://js.stripe.com
- http://ocsp.pki.goog
- http://localhost:3001
- http://r3.o.lencr.org
- http://ocsp.digicert.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%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	2 (13.3%)	2 (13.3%)	0 (0.0%)	4 (26.7%)
	Low	0 (0.0%)	2 (13.3%)	3 (20.0%)	1 (6.7%)	6 (40.0%)
	Informational	0 (0.0%)	1 (6.7%)	3 (20.0%)	1 (6.7%)	5 (33.3%)
	Total	0 (0.0%)	5 (33.3%)	8 (53.3%)	2 (13.3%)	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://m.stripe.com	0 (0)	0 (0)	1 (1)	0 (1)
	https://m.stripe.network	0 (0)	0 (0)	1 (1)	0 (1)
	https://js.stripe.com	0 (0)	1 (1)	1 (2)	2 (4)
	http://ocsp.pki.goog	0 (0)	1 (1)	0 (1)	0 (1)
	http://localhost:3001	0 (0)	2 (2)	1 (3)	2 (5)
	http://ocsp.digicert.com	0 (0)	0 (0)	2 (2)	1 (3)

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	7 (46.7%)
Content Security Policy (CSP) Header Not Set	Medium	4 (26.7%)
Cross-Domain Misconfiguration	Medium	16 (106.7%)
Missing Anti-clickjacking Header	Medium	5 (33.3%)
CSP: Notices	Low	2 (13.3%)
Cookie with SameSite Attribute None	Low	1 (6.7%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	13 (86.7%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	3 (20.0%)
Timestamp Disclosure - Unix	Low	18 (120.0%)
X-Content-Type-Options Header Missing	Low	10 (66.7%)
Total		15

Alert type	Risk	Count
Content Security Policy (CSP) Report-Only Header Found	Informational	1 (6.7%)
Information Disclosure - Suspicious Comments	Informational	19 (126.7%)
Modern Web Application	Informational	6 (40.0%)
Re-examine Cache-control Directives	Informational	3 (20.0%)
Retrieved from Cache	Informational	6 (40.0%)
Total		15

Alerts

Risk=Medium, Confidence=High (2)

https://js.stripe.com (1)

CSP: Wildcard Directive (1)

▶ GET https://js.stripe.com/v3/m-outer-93afeeb17bc37e711759584dbfc50d47.html

http://ocsp.pki.goog (1)

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

▶ GET http://ocsp.pki.goog/gts1c3

Risk=Medium, Confidence=Medium (2)

http://localhost:3001 (2)

Cross-Domain Misconfiguration (1)

▶ GET http://localhost:3001/signin

Missing Anti-clickjacking Header (1)

▶ GET http://localhost:3001/signin

Risk=Low, Confidence=High (2)

https://js.stripe.com (1)

CSP: Notices (1)

▶ GET https://js.stripe.com/v3/m-outer-93afeeb17bc37e711759584dbfc50d47.html

http://ocsp.digicert.com (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▶ GET http://ocsp.digicert.com/

Risk=Low, Confidence=Medium (3)

https://m.stripe.com (1)

Cookie with SameSite Attribute None (1)

▶ POST https://m.stripe.com/6

http://localhost:3001 (1)

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

▶ GET http://localhost:3001/signin

http://ocsp.digicert.com (1)

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

▶ GET http://ocsp.digicert.com/

Risk=Low, Confidence=Low (1)

https://m.stripe.network (1)

Timestamp Disclosure - Unix (1)

▶ GET https://m.stripe.network/out-4.5.42.js

Risk=Informational, Confidence=High (1)

https://js.stripe.com (1)

Content Security Policy (CSP) Report-Only Header Found (1)

▶ GET https://js.stripe.com/v3/m-outer-93afeeb17bc37e711759584dbfc50d47.html

Risk=Informational, Confidence=Medium (3)

http://localhost:3001 (2)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost:3001/signin

Modern Web Application (1)

▶ GET http://localhost:3001/signin

http://ocsp.digicert.com (1)

Retrieved from Cache (1)

▶ GET http://ocsp.digicert.com/

Risk=Informational, Confidence=Low (1)

https://js.stripe.com (1)

Re-examine Cache-control Directives (1)

▶ GET https://js.stripe.com/v3/m-outer-93afeeb17bc37e711759584dbfc50d47.html

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

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 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

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

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200

WASC ID	13
Reference	▪ http://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 ▪ 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

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

Content Security Policy (CSP) Report-Only Header Found

Source raised by a passive scanner (Content Security Policy (CSP) Header Not Set)

CWE ID 693

WASC ID 15

Reference

- https://www.w3.org/TR/CSP2/
- https://w3c.github.io/webappsec-csp/
- http://caniuse.com/#feat=contentsecuritypolicy
- http://content-security-policy.com/

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)