CitiBank-Scan-Report

Generated with ZAP on Tue 6 Dec 2022, at 16:34:58

Contents

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- http://www.citi.com
- https://www.citi.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%)	1 (5.9%)	2 (11.8%)	1 (5.9%)	4 (23.5%)
	Low	0 (0.0%)	2 (11.8%)	5 (29.4%)	1 (5.9%)	8 (47.1%)
	Informational	0 (0.0%)	0 (0.0%)	1 (5.9%)	4 (23.5%)	5 (29.4%)
	Total	0 (0.0%)	3 (17.6%)	8 (47.1%)	6 (35.3%)	17 (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)
https://www.citi.com Site	0 (0)	4 (4)	8 (12)	5 (17)

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
Absence of Anti-CSRF Tokens	Medium	2 (11.8%)
Application Error Disclosure	Medium	1 (5.9%)
Content Security Policy (CSP) Header Not Set	Medium	5 (29.4%)
Missing Anti-clickjacking Header	Medium	3 (17.6%)
Cookie No HttpOnly Flag	Low	5 (29.4%)
Total		17

Alert type	Risk	Count
Cookie Without Secure Flag	Low	1 (5.9%)
Cookie with SameSite Attribute None	Low	1 (5.9%)
Cookie without SameSite Attribute	Low	4 (23.5%)
Strict-Transport-Security Header Not Set	Low	9 (52.9%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	16 (94.1%)
Timestamp Disclosure - Unix	Low	77 (452.9%)
X-Content-Type-Options Header Missing	Low	3 (17.6%)
Information Disclosure - Suspicious Comments	Informational	18 (105.9%)
Loosely Scoped Cookie	Informational	4 (23.5%)
Modern Web Application	Informational	5 (29.4%)
Re-examine Cache-control Directives	Informational	4 (23.5%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	2 (11.8%)
Total		17

Alerts

Risk=Medium, Confidence=High (1)

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

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

▶ GET https://www.citi.com/

Risk=Medium, Confidence=Medium (2)

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

Application Error Disclosure (1)

▶ GET https://www.citi.com/cbol-pre-login-static-assets/main.1b8adb522fbe4fd1.js

Missing Anti-clickjacking Header (1)

▶ GET https://www.citi.com/

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.citi.com/

Risk=Low, Confidence=High (2)

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

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.citi.com/robots.txt

Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec) (1)

▶ GET https://www.citi.com/

Risk=Low, Confidence=Medium (5)

https://www.citi.com (5)

Cookie No HttpOnly Flag (1)

▶ GET https://www.citi.com/robots.txt

Cookie Without Secure Flag (1)

▶ GET https://www.citi.com/assets/scripts/global/6c8322c7341eac98645c10e3d1d3c7ae.js

Cookie with SameSite Attribute None (1)

▶ GET https://www.citi.com/public/342e9cf8d6a1555bf6f96086ea852669dd0011213c3f

Cookie without SameSite Attribute (1)

▶ GET https://www.citi.com/robots.txt

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

▶ GET https://www.citi.com/robots.txt

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.citi.com/assets/scripts/global/6c8322c7341eac98645c10e3d1d3c7ae.js

Risk=Informational, Confidence=Medium (1)

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

Modern Web Application (1)

▶ GET https://www.citi.com/

Risk=Informational, Confidence=Low (4)

https://www.citi.com (4)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.citi.com/

Loosely Scoped Cookie (1)

▶ GET https://www.citi.com/robots.txt

Re-examine Cache-control Directives (1)

▶ GET https://www.citi.com/robots.txt

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

▶ GET https://www.citi.com/?remember=accepted

Appendix

Alert types

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

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

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/

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

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 Without Secure Flag

Source	raised by a passive scanner (Cookie Without Secure Flag)
CWE ID	614
WASC ID	13
Reference	▪ 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

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

Cookie without SameSite Attribute

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

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

Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	- http://tools.ietf.org/html/rfc6797#section-8.1

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 - 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/

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