StandardCharteredBank-Scan-Report

Generated with ZAP on Sat 3 Dec 2022, at 17:10:34

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.sc.com
- https://www.sc.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%)	3 (14.3%)	3 (14.3%)	1 (4.8%)	7 (33.3%)
	Low	0 (0.0%)	2 (9.5%)	6 (28.6%)	1 (4.8%)	9 (42.9%)
	Informational	0 (0.0%)	0 (0.0%)	2 (9.5%)	3 (14.3%)	5 (23.8%)
	Total	0 (0.0%)	5 (23.8%)	11 (52.4%)	5 (23.8%)	21 (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://www.sc.com	0 (0)	7 (7)	9 (16)	5 (21)

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	346 (1,647.6%)
Application Error Disclosure	Medium	1 (4.8%)
CSP: Wildcard Directive	Medium	649 (3,090.5%)
CSP: script-src unsafe-inline	Medium	649 (3,090.5%)
Total		21

Alert type	Risk	Count
CSP: style-src unsafe-inline	Medium	649 (3,090.5%)
Cross-Domain Misconfiguration	Medium	5 (23.8%)
Vulnerable JS Library	Medium	1 (4.8%)
CSP: Notices	Low	1 (4.8%)
Cookie No HttpOnly Flag	Low	1 (4.8%)
Cookie Without Secure Flag	Low	1 (4.8%)
Cookie without SameSite Attribute	Low	2 (9.5%)
Cross-Domain JavaScript Source File Inclusion	Low	1835 (8,738.1%)
Information Disclosure - Debug Error Messages	Low	2 (9.5%)
Strict-Transport-Security Header Not Set	Low	2 (9.5%)
Timestamp Disclosure - Unix	Low	445 (2,119.0%)
X-Content-Type-Options Header Missing	Low	73 (347.6%)
Total		21

Alert type	Risk	Count
Charset Mismatch	Informational	10 (47.6%)
Information Disclosure - Suspicious Comments	Informational	946 (4,504.8%)
Modern Web Application	Informational	674 (3,209.5%)
Re-examine Cache-control Directives	Informational	682 (3,247.6%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	1 (4.8%)
Total		21

Alerts

Risk=Medium, Confidence=High (3)

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

CSP: Wildcard Directive (1)

▶ GET https://www.sc.com/pk/

CSP: script-src unsafe-inline (1)

▶ GET https://www.sc.com/pk/

CSP: style-src unsafe-inline (1)

▶ GET https://www.sc.com/pk/

Risk=Medium, Confidence=Medium (3)

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

Application Error Disclosure (1)

▶ GET https://www.sc.com/en/cookie-policy/

Cross-Domain Misconfiguration (1)

▶ GET https://www.sc.com/pl/content/themes/standard-chartered-non-retail/assets/src/images/site-icons/safari-pinned-tab.svg

Vulnerable JS Library (1)

▶ GET https://www.sc.com/global/av/global-new.js

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.sc.com/en/404/

Risk=Low, Confidence=High (2)

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

CSP: Notices (1)

▶ GET https://www.sc.com/hk/

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.sc.com/se/cookie-policy/

Risk=Low, Confidence=Medium (6)

https://www.sc.com (6)

Cookie No HttpOnly Flag (1)

▶ GET https://www.sc.com/nfs/orr/foa/view_reward_home.htm?ctry=SG&lang=en_SG

Cookie Without Secure Flag (1)

▶ GET https://www.sc.com/nfs/orr/foa/view_reward_home.htm?ctry=SG&lang=en_SG

Cookie without SameSite Attribute (1)

▶ GET https://www.sc.com/nfs/orr/foa/view_reward_home.htm?ctry=SG&lang=en_SG

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.sc.com/pk/

Information Disclosure - Debug Error Messages (1)

▶ GET https://www.sc.com/en/cookie-policy/

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

▶ GET https://www.sc.com/robots.txt

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.sc.com/pk/

Risk=Informational, Confidence=Medium (2)

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

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.sc.com/pk/

Modern Web Application (1)

▶ GET https://www.sc.com/pk/

Risk=Informational, Confidence=Low (3)

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

Charset Mismatch (1)

▶ GET https://www.sc.com/ch/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fwww.sc.com%2Fch%2F

Re-examine Cache-control Directives (1)

▶ GET https://www.sc.com/robots.txt

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

▶ GET https://www.sc.com/en/?s=ZAP

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

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/fundamental

s/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

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

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	▪ https://nvd.nist.gov/vuln/detail/CVE-2012-6708 ▪ https://github.com/jquery/jquery/issues/2432 ▪ http://research.insecurelabs.org/jquery/test/ ▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ ▪ http://bugs.jquery.com/ticket/11290 ▪ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ ▪ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 ▪ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 ▪ https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b ▪ https://bugs.jquery.com/ticket/11974

- https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

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 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 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

Cross-Domain JavaScript Source File Inclusion

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

Information Disclosure - Debug Error Messages

Source	raised by a passive scanner (Information Disclosure - Debug Error Messages)
CWE ID	200
WASC ID	13

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

Charset Mismatch

Source	raised by a passive scanner (Charset Mismatch)
CWE ID	436
WASC ID	15
Reference	▪ http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

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/

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