SoneriBank-Scan-Report

Generated with ZAP on Wed 14 Dec 2022, at 16:07:15

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.soneribank.com
- https://www.soneribank.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%)	1 (4.3%)	1 (4.3%)	0 (0.0%)	2 (8.7%)
	Medium	0 (0.0%)	4 (17.4%)	2 (8.7%)	1 (4.3%)	7 (30.4%)
	Low	0 (0.0%)	2 (8.7%)	3 (13.0%)	1 (4.3%)	6 (26.1%)
	Informational	0 (0.0%)	2 (8.7%)	2 (8.7%)	4 (17.4%)	8 (34.8%)
	Total	0 (0.0%)	9 (39.1%)	8 (34.8%)	6 (26.1%)	23 (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.soneribank.com	2 (2)	7 (9)	6 (15)	8 (23)

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
Hash Disclosure - Mac OSX salted SHA-1	High	3 (13.0%)
PII Disclosure	High	32 (139.1%)
Total		23

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	6990 (30,391.3%)
CSP: Wildcard Directive	Medium	6486 (28,200.0%)
CSP: script-src unsafe-inline	Medium	6486 (28,200.0%)
CSP: style-src unsafe-inline	Medium	6486 (28,200.0%)
Content Security Policy (CSP) Header Not Set	Medium	1 (4.3%)
Multiple X-Frame-Options Header Entries	Medium	2621 (11,395.7%)
Vulnerable JS Library	Medium	4 (17.4%)
Application Error Disclosure	Low	2 (8.7%)
Cookie without SameSite Attribute	Low	1 (4.3%)
Cross-Domain JavaScript Source File Inclusion	Low	395 (1,717.4%)
Strict-Transport-Security Header Not Set	Low	7 (30.4%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	8765 (38,108.7%)
Total		23

Alert type	Risk	Count
Timestamp Disclosure - Unix	Low	445 (1,934.8%)
CSP: X-Content-Security-Policy	Informational	6087 (26,465.2%)
Charset Mismatch	Informational	584 (2,539.1%)
Content Security Policy (CSP) Report-Only Header Found	Informational	319 (1,387.0%)
Information Disclosure - Suspicious Comments	Informational	14684 (63,843.5%)
Modern Web Application	Informational	6128 (26,643.5%)
Re-examine Cache-control Directives	Informational	1567 (6,813.0%)
Retrieved from Cache	Informational	119 (517.4%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	3693 (16,056.5%)
Total		23

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

▶ GET https://www.soneribank.com/wp-content/uploads/2018/11/SNBL-ADT1-TFCs-IPO-Application-Form.pdf

Risk=High, Confidence=Medium (1)

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

Hash Disclosure - Mac OSX salted SHA-1 (1)

▶ GET https://www.soneribank.com/wp-content/uploads/2020/03/Mandate_Form.pdf

Risk=Medium, Confidence=High (4)

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

CSP: Wildcard Directive (1)

▶ GET https://www.soneribank.com/sitemap.xml

CSP: script-src unsafe-inline (1)

▶ GET https://www.soneribank.com/sitemap.xml

CSP: style-src unsafe-inline (1)

▶ GET https://www.soneribank.com/sitemap.xml

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

▶ GET https://www.soneribank.com/cdn-cgi/l/email-protection

Risk=Medium, Confidence=Medium (2)

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

Multiple X-Frame-Options Header Entries (1)

▶ GET https://www.soneribank.com/

Vulnerable JS Library (1)

▶ GET https://www.soneribank.com/wp-content/themes/soneribank/includes/js/libs/jquery.js?ver=1.8.3

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.soneribank.com/

Risk=Low, Confidence=High (2)

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

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.soneribank.com/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js

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

▶ GET https://www.soneribank.com/robots.txt

Risk=Low, Confidence=Medium (3)

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

Application Error Disclosure (1)

▶ GET https://www.soneribank.com/author/admin/

Cookie without SameSite Attribute (1)

▶ GET https://www.soneribank.com/

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.soneribank.com/soneri-digital/

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.soneribank.com/media-center/radio-spot/

Risk=Informational, Confidence=High (2)

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

CSP: X-Content-Security-Policy (1)

▶ GET https://www.soneribank.com/

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

▶ GET https://www.soneribank.com/media-center/radio-spot/

Risk=Informational, Confidence=Medium (2)

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

Modern Web Application (1)

▶ GET https://www.soneribank.com/

Retrieved from Cache (1)

▶ GET https://www.soneribank.com/wp-content/plugins/Mera%20Ghar%20Mera%20Pakistan/css/form.css?ver=6.1.1

Risk=Informational, Confidence=Low (4)

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

Charset Mismatch (1)

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

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.soneribank.com/

Re-examine Cache-control Directives (1)

▶ GET https://www.soneribank.com/robots.txt

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

```
▶ GET https://www.soneribank.com/?
_wp_http_referer=%2F&_wpnonce=4b204e286d&s=ZAP
```

Appendix

Alert types

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

Hash Disclosure - Mac OSX salted SHA-1

Source	raised by a passive scanner (Hash Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage ▪ http://openwall.info/wiki/john/sample-hashes

PII Disclosure

Source	raised by a passive scanner (PII Disclosure)
CWE ID	359
WASC ID	13

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

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/fundamentals/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+p

olicy

- 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/

Multiple X-Frame-Options Header Entries

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	▪ https://tools.ietf.org/html/rfc7034

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/

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

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

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

CSP: X-Content-Security-Policy

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

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

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)

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