SilkBank-Scan-Report

Generated with ZAP on Sun 4 Dec 2022, at 17:48:25

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.silkbank.com.pk`
- `https://www.silkbank.com.pk`

(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 (5.9%)	1 (5.9%)	0 (0.0%)	2 (11.8%)
	Medium	0 (0.0%)	1 (5.9%)	3 (17.6%)	1 (5.9%)	5 (29.4%)
	Low	0 (0.0%)	1 (5.9%)	3 (17.6%)	1 (5.9%)	5 (29.4%)
	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)
Site	http://www.silkbank.com.pk	0 (0)	1 (1)	0 (1)	0 (1)
	https://www.silkbank.com.pk	2 (2)	4 (6)	5 (11)	5 (16)

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	1 (5.9%)
PII Disclosure	High	13 (76.5%)
Total		17

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	594 (3,494.1%)
Content Security Policy (CSP) Header Not Set	Medium	361 (2,123.5%)
Secure Pages Include Mixed Content (Including Scripts)	Medium	3 (17.6%)
Vulnerable JS Library	Medium	8 (47.1%)
Weak Authentication Method	Medium	150 (882.4%)
Cookie without SameSite Attribute	Low	1 (5.9%)
Cross-Domain JavaScript Source File Inclusion	Low	723 (4,252.9%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	894 (5,258.8%)
Timestamp Disclosure - Unix	Low	14 (82.4%)
X-Content-Type-Options Header Missing	Low	1217 (7,158.8%)
Charset Mismatch (Header Versus Meta Charset)	Informational	30 (176.5%)
Information Disclosure - Suspicious Comments	Informational	410 (2,411.8%)
Total		17

Alert type	Risk	Count
Modern Web Application	Informational	343 (2,017.6%)
Re-examine Cache-control Directives	Informational	25 (147.1%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	155 (911.8%)
Total		17

Alerts

Risk=High, Confidence=High (1)

https://www.silkbank.com.pk (1)

PII Disclosure (1)

▶ GET https://www.silkbank.com.pk/pdf/Silkbank%20Disclaimer%20Policy%20(4).pdf

Risk=High, Confidence=Medium (1)

https://www.silkbank.com.pk (1)

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

▶ GET https://www.silkbank.com.pk/admin/upload/PDF/81124-half_yr_2012.pdf

Risk=Medium, Confidence=High (1)

https://www.silkbank.com.pk (1)

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

▶ GET https://www.silkbank.com.pk/

Risk=Medium, Confidence=Medium (3)

http://www.silkbank.com.pk (1)

Weak Authentication Method (1)

▶ GET http://www.silkbank.com.pk/admin/upload/PDF%20Emaan/86361-Ombudsman.pdf

https://www.silkbank.com.pk (2)

Secure Pages Include Mixed Content (Including Scripts) (1)

▶ GET https://www.silkbank.com.pk/alliance/

Vulnerable JS Library (1)

▶ GET https://www.silkbank.com.pk/vendor/bootstrap/js/bootstrap.min.js

Risk=Medium, Confidence=Low (1)

https://www.silkbank.com.pk (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.silkbank.com.pk/

Risk=Low, Confidence=High (1)

https://www.silkbank.com.pk (1)

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

▶ GET https://www.silkbank.com.pk/robots.txt

Risk=Low, Confidence=Medium (3)

https://www.silkbank.com.pk (3)

Cookie without SameSite Attribute (1)

▶ GET https://www.silkbank.com.pk/

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.silkbank.com.pk/

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

▶ GET https://www.silkbank.com.pk/robots.txt

Risk=Low, Confidence=Low (1)

https://www.silkbank.com.pk (1)

Timestamp Disclosure - Unix (1)

▶ GET `https://www.silkbank.com.pk/img/silkFavicon/apple-icon-57x57.png`

Risk=Informational, Confidence=Medium (1)

https://www.silkbank.com.pk (1)

Modern Web Application (1)

▶ GET `https://www.silkbank.com.pk/`

Risk=Informational, Confidence=Low (4)

https://www.silkbank.com.pk (4)

Charset Mismatch (Header Versus Meta Charset) (1)

▶ GET `https://www.silkbank.com.pk/urdu/status-of-the-company/`

Information Disclosure - Suspicious Comments (1)

▶ GET `https://www.silkbank.com.pk/`

Re-examine Cache-control Directives (1)

▶ GET `https://www.silkbank.com.pk/robots.txt`

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

▶ GET `https://www.silkbank.com.pk/pages/careers/?sbl=70`

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

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/

Secure Pages Include Mixed Content (Including Scripts)

Source	raised by a passive scanner (Secure Pages Include Mixed Content)

CWE ID	311
WASC ID	4
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	▪ https://github.com/twbs/bootstrap/issues/28236 ▪ https://github.com/twbs/bootstrap/issues/20184 ▪ https://github.com/advisories/GHSA-4p24-vmcr-4gqj

Weak Authentication Method

Source	raised by a passive scanner (Weak Authentication Method)
CWE ID	326
WASC ID	4
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.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

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

Charset Mismatch (Header Versus Meta Charset)

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