SummitBank-Scan-Report

Generated with ZAP on Tue 13 Dec 2022, at 19:44:29

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://summitbank.com.pk
- https://summitbank.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 (4.5%)	0 (0.0%)	0 (0.0%)	1 (4.5%)
	Medium	0 (0.0%)	4 (18.2%)	2 (9.1%)	1 (4.5%)	7 (31.8%)
	Low	0 (0.0%)	1 (4.5%)	5 (22.7%)	1 (4.5%)	7 (31.8%)
	Informational	0 (0.0%)	0 (0.0%)	2 (9.1%)	5 (22.7%)	7 (31.8%)
	Total	0 (0.0%)	6 (27.3%)	9 (40.9%)	7 (31.8%)	22 (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.)

Site	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
http://summitbank.com.pk	1 (1)	1 (2)	1 (3)	0 (3)
https://summitbank.com.pk	0 (0)	6 (6)	6 (12)	7 (19)

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
PII Disclosure	High	14 (63.6%)
Absence of Anti-CSRF Tokens	Medium	196 (890.9%)
CSP: Wildcard Directive	Medium	245 (1,113.6%)
Total		22

Alert type	Risk	Count
CSP: script-src unsafe-inline	Medium	245 (1,113.6%)
CSP: style-src unsafe-inline	Medium	245 (1,113.6%)
Content Security Policy (CSP) Header Not Set	Medium	53 (240.9%)
Secure Pages Include Mixed Content (Including Scripts)	Medium	151 (686.4%)
Vulnerable JS Library	Medium	9 (40.9%)
Cookie No HttpOnly Flag	Low	473 (2,150.0%)
Cookie Without Secure Flag	Low	304 (1,381.8%)
Cookie without SameSite Attribute	Low	473 (2,150.0%)
Cross-Domain JavaScript Source File Inclusion	Low	3 (13.6%)
Private IP Disclosure	Low	14 (63.6%)
Strict-Transport-Security Header Not Set	Low	417 (1,895.5%)
Timestamp Disclosure - Unix	Low	3 (13.6%)
Total		22

Alert type	Risk	Count
Charset Mismatch	Informational	32 (145.5%)
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	2 (9.1%)
Cookie Poisoning	Informational	47 (213.6%)
Information Disclosure - Suspicious Comments	Informational	257 (1,168.2%)
Modern Web Application	Informational	203 (922.7%)
Re-examine Cache-control Directives	Informational	222 (1,009.1%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	27 (122.7%)
Total		22

Alerts

Risk=High, Confidence=High (1)

http://summitbank.com.pk (1)

PII Disclosure (1)

▶ GET http://summitbank.com.pk/wp-content/uploads/2019/07/CP-SelfCertForm-v4-U.pdf

Risk=Medium, Confidence=High (4)

http://summitbank.com.pk (1)

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

▶ GET http://summitbank.com.pk/?lang=ur

https://summitbank.com.pk (3)

CSP: Wildcard Directive (1)

▶ GET https://summitbank.com.pk/

CSP: script-src unsafe-inline (1)

▶ GET https://summitbank.com.pk/

CSP: style-src unsafe-inline (1)

▶ GET https://summitbank.com.pk/

Risk=Medium, Confidence=Medium (2)

https://summitbank.com.pk (2)

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

▶ GET https://summitbank.com.pk/about-us/

Vulnerable JS Library (1)

▶ GET https://summitbank.com.pk/testiban/js/jquery-1.2.6.pack.js

Risk=Medium, Confidence=Low (1)

https://summitbank.com.pk (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://summitbank.com.pk/testiban/iban-new.php

Risk=Low, Confidence=High (1)

https://summitbank.com.pk (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://summitbank.com.pk/sitemap.xml

Risk=Low, Confidence=Medium (5)

http://summitbank.com.pk (1)

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET http://summitbank.com.pk/branch-locator/

https://summitbank.com.pk (4)

Cookie No HttpOnly Flag (1)

▶ GET https://summitbank.com.pk/robots.txt

Cookie Without Secure Flag (1)

▶ GET https://summitbank.com.pk/robots.txt

Cookie without SameSite Attribute (1)

▶ GET https://summitbank.com.pk/robots.txt

Private IP Disclosure (1)

▶ GET https://summitbank.com.pk/testiban/iban-new.php

Risk=Low, Confidence=Low (1)

https://summitbank.com.pk (1)

Timestamp Disclosure - Unix (1)

▶ GET https://summitbank.com.pk/wp-content/themes/awaken/css/bootstrap.min.css?ver=all

Risk=Informational, Confidence=Medium (2)

https://summitbank.com.pk (2)

Information Disclosure - Suspicious Comments (1)

▶ GET https://summitbank.com.pk/about-us/

Modern Web Application (1)

▶ GET https://summitbank.com.pk/testiban/iban-new.php

Risk=Informational, Confidence=Low (5)

https://summitbank.com.pk (5)

Charset Mismatch (1)

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

Charset Mismatch (Header Versus Meta Content-Type Charset) (1)

▶ GET https://summitbank.com.pk/testiban/iban-new.php

Cookie Poisoning (1)

▶ GET https://summitbank.com.pk/about-us/?lang=ur

Re-examine Cache-control Directives (1)

▶ GET https://summitbank.com.pk/robots.txt

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

▶ GET https://summitbank.com.pk/about-us/?lang=ur

Appendix

Alert types

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

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/

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://nvd.nist.gov/vuln/detail/CVE-2012-6708 - http://research.insecurelabs.org/jquery/test/ - https://bugs.jquery.com/ticket/9521 - 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://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b

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

- https://nvd.nist.gov/vuln/detail/CVE-2011-4969

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

Private IP Disclosure

Source	raised by a passive scanner (Private IP Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ https://tools.ietf.org/html/rfc1918

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

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

Charset Mismatch (Header Versus Meta Content-Type 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

Cookie Poisoning

Source raised by a passive scanner (Cookie Poisoning)

CWE ID 20

WASC ID 20

Reference
- http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-cookie

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