KPKBank-Scan-Report

Generated with ZAP on Mon 5 Dec 2022, at 21:59:36

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.bok.com.pk
- https://www.bok.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 (4.2%)	1 (4.2%)	0 (0.0%)	2 (8.3%)
	Medium	0 (0.0%)	3 (12.5%)	2 (8.3%)	1 (4.2%)	6 (25.0%)
	Low	0 (0.0%)	1 (4.2%)	8 (33.3%)	1 (4.2%)	10 (41.7%)
	Informational	0 (0.0%)	2 (8.3%)	1 (4.2%)	3 (12.5%)	6 (25.0%)
	Total	0 (0.0%)	7 (29.2%)	12 (50.0%)	5 (20.8%)	24 (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.bok.com.pk	2 (2)	6 (8)	10 (18)	6 (24)

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	20 (83.3%)
PII Disclosure	High	71 (295.8%)
Total		24

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	7838 (32,658.3%)
CSP: Wildcard Directive	Medium	4061 (16,920.8%)
CSP: script-src unsafe-inline	Medium	4061 (16,920.8%)
CSP: style-src unsafe-inline	Medium	4061 (16,920.8%)
Multiple X-Frame-Options Header Entries	Medium	1339 (5,579.2%)
Vulnerable JS Library	Medium	4 (16.7%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	351 (1,462.5%)
CSP: Notices	Low	4061 (16,920.8%)
Cookie No HttpOnly Flag	Low	1 (4.2%)
Cookie Without Secure Flag	Low	1 (4.2%)
Cookie with SameSite Attribute None	Low	3 (12.5%)
Cookie without SameSite Attribute	Low	1 (4.2%)
Total		24

Alert type	Risk	Count
Cross-Domain JavaScript Source File Inclusion	Low	3816 (15,900.0%)
Private IP Disclosure	Low	1 (4.2%)
Secure Pages Include Mixed Content	Low	4 (16.7%)
Timestamp Disclosure - Unix	Low	3 (12.5%)
CSP: X-Content-Security-Policy	Informational	4061 (16,920.8%)
CSP: X-WebKit-CSP	Informational	4061 (16,920.8%)
Information Disclosure - Suspicious Comments	Informational	6468 (26,950.0%)
Modern Web Application	Informational	3781 (15,754.2%)
Re-examine Cache-control Directives	Informational	1429 (5,954.2%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	3077 (12,820.8%)
Total		24

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

▶ GET https://www.bok.com.pk/sites/default/files/2021-09/IRRPolicy.pdf

Risk=High, Confidence=Medium (1)

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

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

▶ GET https://www.bok.com.pk/sites/default/files/downloads/pdf/Profit%20rates%20effective%20from%201.07.16%20to%2031.12.16.pdf

Risk=Medium, Confidence=High (3)

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

CSP: Wildcard Directive (1)

▶ GET https://www.bok.com.pk/

CSP: script-src unsafe-inline (1)

▶ GET https://www.bok.com.pk/

CSP: style-src unsafe-inline (1)

▶ GET https://www.bok.com.pk/

Risk=Medium, Confidence=Medium (2)

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

Multiple X-Frame-Options Header Entries (1)

▶ GET https://www.bok.com.pk/

Vulnerable JS Library (1)

▶ GET https://www.bok.com.pk/sites/default/files/js/js_o6yxZaLrST3VwPWbGqZwgfraeFW1ewr5bE3qm0omZ2A.js

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.bok.com.pk/

Risk=Low, Confidence=High (1)

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

CSP: Notices (1)

▶ GET https://www.bok.com.pk/

Risk=Low, Confidence=Medium (8)

https://www.bok.com.pk (8)

Big Redirect Detected (Potential Sensitive Information Leak) (1)

▶ GET https://www.bok.com.pk/search/

Cookie No HttpOnly Flag (1)

▶ GET https://www.bok.com.pk/big_pipe/no-js?destination=/board-of-directors

Cookie Without Secure Flag (1)

▶ GET https://www.bok.com.pk/big_pipe/no-js?destination=/board-of-directors

Cookie with SameSite Attribute None (1)

▶ POST https://www.bok.com.pk/newsletter/validate

Cookie without SameSite Attribute (1)

▶ GET https://www.bok.com.pk/big_pipe/no-js?destination=/board-of-directors

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.bok.com.pk/

Private IP Disclosure (1)

▶ GET https://www.bok.com.pk/sites/default/files/2021-04/Profit%20-%20loss%20Distribution%20Policy%20amended%20140th%20BOD%20meeting%2024-10-2016.pdf

Secure Pages Include Mixed Content (1)

▶ GET https://www.bok.com.pk/islamic/personal-banking/deposit-accounts/term-deposits/riba-free-special-deposit-scheme

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.bok.com.pk/sites/default/files/2021-04/Annual%20Report%202016_1.pdf

Risk=Informational, Confidence=High (2)

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

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

▶ GET https://www.bok.com.pk/

CSP: X-WebKit-CSP (1)

▶ GET https://www.bok.com.pk/

Risk=Informational, Confidence=Medium (1)

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

Modern Web Application (1)

▶ GET https://www.bok.com.pk/

Risk=Informational, Confidence=Low (3)

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

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.bok.com.pk/

Re-examine Cache-control Directives (1)

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

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

▶ POST https://www.bok.com.pk/

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+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

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://bugs.jqueryui.com/ticket/15284 • https://nvd.nist.gov/vuln/detail/CVE-2022-31160 • https://github.com/jquery/jquery-ui/security/advisories/GHSA-h6gj-6jjq-h8g9 • https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327 • https://nvd.nist.gov/vuln/detail/CVE-2021-41184 • https://nvd.nist.gov/vuln/detail/CVE-2021-41183 • https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc • https://nvd.nist.gov/vuln/detail/CVE-2021-41182

Big Redirect Detected (Potential Sensitive Information Leak)

Source	raised by a passive scanner (Big Redirect Detected (Potential Sensitive Information Leak))
CWE ID	201
WASC ID	13

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 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

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

Secure Pages Include Mixed Content

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

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

CSP: X-WebKit-CSP

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

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