HBFCBank-Scan-Report

Generated with ZAP on Tue 6 Dec 2022, at 14:39:29

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://hbfc.com.pk
- https://hbfc.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 (6.2%)	0 (0.0%)	0 (0.0%)	1 (6.2%)
	Medium	0 (0.0%)	1 (6.2%)	3 (18.8%)	1 (6.2%)	5 (31.2%)
	Low	0 (0.0%)	1 (6.2%)	4 (25.0%)	1 (6.2%)	6 (37.5%)
	Informational	0 (0.0%)	0 (0.0%)	2 (12.5%)	2 (12.5%)	4 (25.0%)
	Total	0 (0.0%)	3 (18.8%)	9 (56.2%)	4 (25.0%)	16 (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://hbfc.com.pk	1 (1)	5 (6)	6 (12)	4 (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
PII Disclosure	High	2 (12.5%)
Absence of Anti-CSRF Tokens	Medium	385 (2,406.2%)
Application Error Disclosure	Medium	23 (143.8%)
Content Security Policy (CSP) Header Not Set	Medium	373 (2,331.2%)
Total		16

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	22 (137.5%)
Vulnerable JS Library	Medium	1 (6.2%)
Cookie Without Secure Flag	Low	4 (25.0%)
Cookie without SameSite Attribute	Low	4 (25.0%)
Cross-Domain JavaScript Source File Inclusion	Low	1244 (7,775.0%)
Information Disclosure - Debug Error Messages	Low	23 (143.8%)
Strict-Transport-Security Header Not Set	Low	5 (31.2%)
Timestamp Disclosure - Unix	Low	4 (25.0%)
Information Disclosure - Suspicious Comments	Informational	624 (3,900.0%)
Modern Web Application	Informational	323 (2,018.8%)
Re-examine Cache-control Directives	Informational	18 (112.5%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	82 (512.5%)
Total		16

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

▶ GET https://hbfc.com.pk/page/assets/videos/hbfc%20video%203%2006112020.mp4

Risk=Medium, Confidence=High (1)

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

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

▶ GET https://hbfc.com.pk/robots.txt

Risk=Medium, Confidence=Medium (3)

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

Application Error Disclosure (1)

▶ GET https://hbfc.com.pk/admin/uploads/job/https:/www.hbfc.com.pk/admin/uploads/media/HBFC%20-CAREER-%2023X4.pdf

Missing Anti-clickjacking Header (1)

▶ GET https://hbfc.com.pk/admin/uploads/job/https:/www.hbfc.com.pk/admi

n/uploads/media/HBFC%20-CAREER-%2023X4.pdf

Vulnerable JS Library (1)

▶ GET https://hbfc.com.pk/assets/js/jquery.min.js

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://hbfc.com.pk/

Risk=Low, Confidence=High (1)

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

Strict-Transport-Security Header Not Set (1)

▶ GET https://hbfc.com.pk/admin/uploads/news/

Risk=Low, Confidence=Medium (4)

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

Cookie Without Secure Flag (1)

▶ GET https://hbfc.com.pk/

Cookie without SameSite Attribute (1)

▶ GET https://hbfc.com.pk/

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://hbfc.com.pk/

Information Disclosure - Debug Error Messages (1)

▶ GET https://hbfc.com.pk/admin/uploads/job/https:/hbfc.com.pk/admin/uploads/media/HBFC%20-CAREER-%2023X4.pdf

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://hbfc.com.pk/page/customers/e_tracking

Risk=Informational, Confidence=Medium (2)

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

Information Disclosure - Suspicious Comments (1)

▶ GET https://hbfc.com.pk/

Modern Web Application (1)

▶ GET https://hbfc.com.pk/

Risk=Informational, Confidence=Low (2)

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

Re-examine Cache-control Directives (1)

▶ GET https://hbfc.com.pk/sitemap.xml

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

▶ POST https://hbfc.com.pk/page/customers/online_complaint_form

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

Application Error Disclosure

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

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/

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	• https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	• https://github.com/jquery/jquery/issues/2432 • http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ • http://research.insecurelabs.org/jquery/test/ • 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/

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

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