MCBIslamicBank-Scan-Report

Generated with ZAP on Tue 13 Dec 2022, at 18:43:54

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.mcbislamicbank.com
- https://www.mcbislamicbank.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 (5.9%)	0 (0.0%)	0 (0.0%)	1 (5.9%)
	Medium	0 (0.0%)	1 (5.9%)	3 (17.6%)	1 (5.9%)	5 (29.4%)
	Low	0 (0.0%)	1 (5.9%)	6 (35.3%)	1 (5.9%)	8 (47.1%)
	Informational	0 (0.0%)	0 (0.0%)	1 (5.9%)	2 (11.8%)	3 (17.6%)
	Total	0 (0.0%)	3 (17.6%)	10 (58.8%)	4 (23.5%)	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	https://www.mcbislamicbank.com	1 (1)	5 (6)	8 (14)	3 (17)

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	1 (5.9%)
Absence of Anti-CSRF Tokens	Medium	197 (1,158.8%)
Content Security Policy (CSP) Header Not Set	Medium	960 (5,647.1%)
Total		17

Alert type	Risk	Count
Cross-Domain Misconfiguration	Medium	1150 (6,764.7%)
Missing Anti-clickjacking Header	Medium	911 (5,358.8%)
Vulnerable JS Library	Medium	3 (17.6%)
Cookie No HttpOnly Flag	Low	961 (5,652.9%)
Cookie Without Secure Flag	Low	1641 (9,652.9%)
Cookie without SameSite Attribute	Low	2 (11.8%)
Cross-Domain JavaScript Source File Inclusion	Low	101 (594.1%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	52 (305.9%)
Strict-Transport-Security Header Not Set	Low	1147 (6,747.1%)
Timestamp Disclosure - Unix	Low	1901 (11,182.4%)
X-Content-Type-Options Header Missing	Low	1143 (6,723.5%)
Information Disclosure - Suspicious Comments	Informational	1080 (6,352.9%)
Total		17

Alert type	Risk	Count
Loosely Scoped Cookie	Informational	2 (11.8%)
Modern Web Application	Informational	971 (5,711.8%)
Total		17

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

▶ POST https://www.mcbislamicbank.com/suggestion-complaint/

Risk=Medium, Confidence=High (1)

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

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

▶ GET https://www.mcbislamicbank.com/

Risk=Medium, Confidence=Medium (3)

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

Cross-Domain Misconfiguration (1)

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

Missing Anti-clickjacking Header (1)

▶ GET https://www.mcbislamicbank.com/islamic-banking/

Vulnerable JS Library (1)

▶ GET https://www.mcbislamicbank.com/wp-content/themes/mcbislamic/assets/js/jquery.min.js

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.mcbislamicbank.com/

Risk=Low, Confidence=High (1)

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

Strict-Transport-Security Header Not Set (1)

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

Risk=Low, Confidence=Medium (6)

https://www.mcbislamicbank.com (6)

Cookie No HttpOnly Flag (1)

▶ GET https://www.mcbislamicbank.com/

Cookie Without Secure Flag (1)

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

Cookie without SameSite Attribute (1)

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

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.mcbislamicbank.com/

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

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

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

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

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

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

Risk=Informational, Confidence=Medium (1)

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

Modern Web Application (1)

▶ GET https://www.mcbislamicbank.com/

Risk=Informational, Confidence=Low (2)

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

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.mcbislamicbank.com/

Loosely Scoped Cookie (1)

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

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

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/

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264
WASC ID	14
Reference	• https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

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 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

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))

CWE ID	200
WASC ID	13
Reference	▪ http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx ▪ http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

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

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

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
WASC ID	13

Loosely Scoped Cookie

Source	raised by a passive scanner (Loosely Scoped Cookie)
CWE ID	565
WASC ID	15
Reference	▪ https://tools.ietf.org/html/rfc6265#section-4.1 ▪ 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 ▪ http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)