DubaiIslamicBank-Scan-Report

Generated with ZAP on Sat 3 Dec 2022, at 15:32:07

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.dib.ae
- https://www.dib.ae

(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 (3.7%)	1 (3.7%)	0 (0.0%)	2 (7.4%)
	Medium	0 (0.0%)	4 (14.8%)	3 (11.1%)	1 (3.7%)	8 (29.6%)
	Low	0 (0.0%)	2 (7.4%)	8 (29.6%)	1 (3.7%)	11 (40.7%)
	Informational	0 (0.0%)	1 (3.7%)	1 (3.7%)	4 (14.8%)	6 (22.2%)
	Total	0 (0.0%)	8 (29.6%)	13 (48.1%)	6 (22.2%)	27 (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.dib.ae	2 (2)	8 (10)	11 (21)	6 (27)

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	5 (18.5%)
PII Disclosure	High	65 (240.7%)
Total		27

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	13 (48.1%)
CSP: Wildcard Directive	Medium	839 (3,107.4%)
CSP: script-src unsafe-inline	Medium	839 (3,107.4%)
CSP: style-src unsafe-inline	Medium	839 (3,107.4%)
Content Security Policy (CSP) Header Not Set	Medium	8 (29.6%)
Missing Anti-clickjacking Header	Medium	8 (29.6%)
Multiple X-Frame-Options Header Entries	Medium	461 (1,707.4%)
Vulnerable JS Library	Medium	5 (18.5%)
Cookie No HttpOnly Flag	Low	4678 (17,325.9%)
Cookie Without Secure Flag	Low	4681 (17,337.0%)
Cookie without SameSite Attribute	Low	4681 (17,337.0%)
Cross-Domain JavaScript Source File Inclusion	Low	1192 (4,414.8%)
Total		27

Alert type	Risk	Count
Information Disclosure - Debug Error Messages	Low	3 (11.1%)
Private IP Disclosure	Low	2 (7.4%)
Secure Pages Include Mixed Content	Low	1 (3.7%)
Strict-Transport-Security Header Not Set	Low	10 (37.0%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	2335 (8,648.1%)
Timestamp Disclosure - Unix	Low	31 (114.8%)
X-Content-Type-Options Header Missing	Low	8 (29.6%)
CSP: X-Content-Security-Policy	Informational	839 (3,107.4%)
Information Disclosure - Suspicious Comments	Informational	45 (166.7%)
Loosely Scoped Cookie	Informational	2439 (9,033.3%)
Modern Web Application	Informational	802 (2,970.4%)
Re-examine Cache-control Directives	Informational	526 (1,948.1%)
Total		27

Alert type	Risk	Count
User Controllable HTML Element Attribute (Potential XSS)	Informational	426 (1,577.8%)
Total		27

Alerts

Risk=High, Confidence=High (1)

https://www.dib.ae (1)

PII Disclosure (1)

▶ GET https://www.dib.ae/docs/default-source/sharia-certificates/8-sc-dubai-islamic-credit-cards-al-islami-credit-card.pdf

Risk=High, Confidence=Medium (1)

https://www.dib.ae (1)

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

▶ GET https://www.dib.ae/docs/default-source/financial-reports/dib_1q2020_ir-presentation-full.pdf?sfvrsn=38a9daba_8

Risk=Medium, Confidence=High (4)

https://www.dib.ae (4)

CSP: Wildcard Directive (1)

▶ GET https://www.dib.ae/sitemap.xml

CSP: script-src unsafe-inline (1)

▶ GET https://www.dib.ae/sitemap.xml

CSP: style-src unsafe-inline (1)

▶ GET https://www.dib.ae/sitemap.xml

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

▶ GET https://www.dib.ae/global/%7B%7BAnswerthumbnail.Url%7D%7D

Risk=Medium, Confidence=Medium (3)

https://www.dib.ae (3)

Missing Anti-clickjacking Header (1)

▶ GET https://www.dib.ae/global/%7B%7BAnswerthumbnail.Url%7D%7D

Multiple X-Frame-Options Header Entries (1)

▶ GET https://www.dib.ae/

Vulnerable JS Library (1)

▶ GET https://www.dib.ae/ScriptResource.axd?d=EydukmxBmDstn7gSYzQESLze-0UBx6BIzs45Gi5Zn50HVrwxbx0CG4NmmOLv4FDgEsZ0Vwv51Y-J3LeN2rw2UrsofmH9Da7LV7rIgzyPrb5kPmGjkYhAgEY_YqpfWRfBUzp8j-U0NqqfvliB4oqtGFwmHuz4G2FNra0cyA4Azv1iCZb_0&t=60f80fc6

Risk=Medium, Confidence=Low (1)

https://www.dib.ae (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.dib.ae/global/iban-validator

Risk=Low, Confidence=High (2)

https://www.dib.ae (2)

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.dib.ae/global/%7B%7BAnswerthumbnail.Url%7D%7D

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

▶ GET https://www.dib.ae/robots.txt

Risk=Low, Confidence=Medium (8)

https://www.dib.ae (8)

Cookie No HttpOnly Flag (1)

▶ GET https://www.dib.ae/robots.txt

Cookie Without Secure Flag (1)

▶ GET https://www.dib.ae/robots.txt

Cookie without SameSite Attribute (1)

▶ GET https://www.dib.ae/robots.txt

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.dib.ae/sitemap.xml

Information Disclosure - Debug Error Messages (1)

▶ GET https://www.dib.ae/personal/home-finance/first-time-buyers

Private IP Disclosure (1)

▶ GET https://www.dib.ae/images/default-source/default-album/listing_advance_wakala_enx.jpg?sfvrsn=adeba79d_54

Secure Pages Include Mixed Content (1)

▶ GET https://www.dib.ae/offers/card-offers/20-cashback

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

▶ GET https://www.dib.ae/global/%7B%7BAnswerthumbnail.Url%7D%7D

Risk=Low, Confidence=Low (1)

https://www.dib.ae (1)

Timestamp Disclosure - Unix (1)

▶ GET https://www.dib.ae/images/default-source/spotlight/8997-travel-spends-hpsl-eng.jpg?sfvrsn=fa2f7113_4)

Risk=Informational, Confidence=High (1)

https://www.dib.ae (1)

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

▶ GET https://www.dib.ae/sitemap.xml

Risk=Informational, Confidence=Medium (1)

https://www.dib.ae (1)

Modern Web Application (1)

▶ GET https://www.dib.ae/sitemap.xml

Risk=Informational, Confidence=Low (4)

https://www.dib.ae (4)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.dib.ae/global/branch-atm-locator

Loosely Scoped Cookie (1)

▶ GET https://www.dib.ae/robots.txt

Re-examine Cache-control Directives (1)

▶ GET https://www.dib.ae/robots.txt

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

▶ GET https://www.dib.ae/global/calculator/finance?type=finance

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

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

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	▪ http://research.insecurelabs.org/jquery/test/ ▪ http://bugs.jquery.com/ticket/11290

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

Information Disclosure - Debug Error Messages

Source	raised by a passive scanner (Information Disclosure - Debug Error Messages)
CWE ID	200
WASC ID	13

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

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

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

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

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)

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