HabibMetroBank-Scan-Report

Generated with ZAP on Sun 4 Dec 2022, at 20:22:09

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.habibmetro.com
- https://www.habibmetro.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 (4.3%)	1 (4.3%)	0 (0.0%)	2 (8.7%)
	Medium	0 (0.0%)	4 (17.4%)	2 (8.7%)	1 (4.3%)	7 (30.4%)
	Low	0 (0.0%)	1 (4.3%)	6 (26.1%)	1 (4.3%)	8 (34.8%)
	Informational	0 (0.0%)	0 (0.0%)	2 (8.7%)	4 (17.4%)	6 (26.1%)
	Total	0 (0.0%)	6 (26.1%)	11 (47.8%)	6 (26.1%)	23 (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.habibmetro.com	2 (2)	7 (9)	8 (17)	6 (23)

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	1 (4.3%)
PII Disclosure	High	20 (87.0%)
Total		23

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	2773 (12,056.5%)
CSP: Wildcard Directive	Medium	1322 (5,747.8%)
CSP: script-src unsafe-inline	Medium	1322 (5,747.8%)
CSP: style-src unsafe-inline	Medium	1322 (5,747.8%)
Content Security Policy (CSP) Header Not Set	Medium	4 (17.4%)
Cross-Domain Misconfiguration	Medium	2927 (12,726.1%)
Vulnerable JS Library	Medium	7 (30.4%)
CSP: Notices	Low	1429 (6,213.0%)
Cookie No HttpOnly Flag	Low	1 (4.3%)
Cookie Without Secure Flag	Low	1 (4.3%)
Cookie without SameSite Attribute	Low	1 (4.3%)
Cross-Domain JavaScript Source File Inclusion	Low	2502 (10,878.3%)
Total		23

Alert type	Risk	Count
Private IP Disclosure	Low	7 (30.4%)
Secure Pages Include Mixed Content	Low	17 (73.9%)
Timestamp Disclosure - Unix	Low	843 (3,665.2%)
Charset Mismatch	Informational	254 (1,104.3%)
Content-Type Header Missing	Informational	1 (4.3%)
Information Disclosure - Suspicious Comments	Informational	2933 (12,752.2%)
Modern Web Application	Informational	964 (4,191.3%)
Re-examine Cache-control Directives	Informational	963 (4,187.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	3221 (14,004.3%)
Total		23

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

▶ GET https://www.habibmetro.com/wp-content/uploads/2022/03/HabibMetro-Code-of-Conduct-For-Website.pdf

Risk=High, Confidence=Medium (1)

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

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

▶ GET https://www.habibmetro.com/wp-content/uploads/2021/07/Consolidated_Accounts-2006.pdf

Risk=Medium, Confidence=High (4)

https://www.habibmetro.com (4)

CSP: Wildcard Directive (1)

▶ GET https://www.habibmetro.com/wp-admin/

CSP: script-src unsafe-inline (1)

▶ GET https://www.habibmetro.com/wp-admin/

CSP: style-src unsafe-inline (1)

▶ GET https://www.habibmetro.com/wp-admin/

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

▶ GET https://www.habibmetro.com/wp-includes/

Risk=Medium, Confidence=Medium (2)

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

Cross-Domain Misconfiguration (1)

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

Vulnerable JS Library (1)

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

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.habibmetro.com/

Risk=Low, Confidence=High (1)

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

CSP: Notices (1)

▶ GET https://www.habibmetro.com/wp-admin/

Risk=Low, Confidence=Medium (6)

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

Cookie No HttpOnly Flag (1)

▶ POST https://www.habibmetro.com/customer-charter/complaint/

Cookie Without Secure Flag (1)

▶ POST https://www.habibmetro.com/customer-charter/complaint/

Cookie without SameSite Attribute (1)

▶ POST https://www.habibmetro.com/customer-charter/complaint/

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.habibmetro.com/

Private IP Disclosure (1)

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

Secure Pages Include Mixed Content (1)

▶ GET https://www.habibmetro.com/sirat/current-accounts/sirat-current-plus-account/

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.habibmetro.com/

Risk=Informational, Confidence=Medium (2)

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

Content-Type Header Missing (1)

▶ GET https://www.habibmetro.com/wp-content/plugins/revslider/public/assets/fonts/font-awesome/fonts/fontawesome-webfont.woff2?v=4.7.0

Modern Web Application (1)

▶ GET https://www.habibmetro.com/

Risk=Informational, Confidence=Low (4)

https://www.habibmetro.com (4)

Charset Mismatch (1)

▶ GET https://www.habibmetro.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fwww.habibmetro.com%2F

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.habibmetro.com/

Re-examine Cache-control Directives (1)

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

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

▶ GET https://www.habibmetro.com/?post_type=page&s=ZAP

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/fundamental

s/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/

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

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/

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 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

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

Content-Type Header Missing

Source	raised by a passive scanner (Content-Type Header Missing)
CWE ID	345
WASC ID	12
Reference	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx

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