XiaomiStoreClone-Scan-Report

Generated with ZAP on Tue 15 Nov 2022, at 22:19:52

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://localhost:8080
- https://i01.appmifile.com
- http://localhost:3000
- https://i02.appmifile.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%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	2 (16.7%)	2 (16.7%)	1 (8.3%)	5 (41.7%)
	Low	0 (0.0%)	0 (0.0%)	3 (25.0%)	0 (0.0%)	3 (25.0%)
	Informational	0 (0.0%)	0 (0.0%)	1 (8.3%)	3 (25.0%)	4 (33.3%)
	Total	0 (0.0%)	2 (16.7%)	6 (50.0%)	4 (33.3%)	12 (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	http://localhost:8080	0 (0)	3 (3)	1 (4)	4 (8)
	http://localhost:3000	0 (0)	2 (2)	2 (4)	0 (4)

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
Absence of Anti-CSRF Tokens	Medium	4 (33.3%)
CSP: Wildcard Directive	Medium	2 (16.7%)
Content Security Policy (CSP) Header Not Set	Medium	6 (50.0%)
Missing Anti-clickjacking Header	Medium	2 (16.7%)
Total		12

Alert type	Risk	Count
Vulnerable JS Library	Medium	2 (16.7%)
Cookie without SameSite Attribute	Low	3 (25.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	10 (83.3%)
X-Content-Type-Options Header Missing	Low	8 (66.7%)
Information Disclosure - Suspicious Comments	Informational	25 (208.3%)
Loosely Scoped Cookie	Informational	2 (16.7%)
Modern Web Application	Informational	6 (50.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	6 (50.0%)
Total		12

Alerts

Risk=Medium, Confidence=High (2)

http://localhost:8080 (1)

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

▶ GET http://localhost:8080/index

http://localhost:3000 (1)

CSP: Wildcard Directive (1)

▶ GET http://localhost:3000/robots.txt

Risk=Medium, Confidence=Medium (2)

http://localhost:8080 (1)

Vulnerable JS Library (1)

▶ GET http://localhost:8080/js/jquery.js

http://localhost:3000 (1)

Missing Anti-clickjacking Header (1)

▶ GET http://localhost:3000

Risk=Medium, Confidence=Low (1)

http://localhost:8080 (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://localhost:8080/index

Risk=Low, Confidence=Medium (3)

http://localhost:8080 (1)

Cookie without SameSite Attribute (1)

▶ GET http://localhost:8080/robots.txt

http://localhost:3000 (2)

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

▶ GET http://localhost:3000

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

▶ GET http://localhost:3000

Risk=Informational, Confidence=Medium (1)

http://localhost:8080 (1)

Modern Web Application (1)

▶ GET http://localhost:8080/js/jquery.js

Risk=Informational, Confidence=Low (3)

http://localhost:8080 (3)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost:8080/js/jquery.easing.min.js

Loosely Scoped Cookie (1)

▶ GET http://localhost:8080/robots.txt

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

▶ POST http://localhost:8080/signup

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

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

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 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

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

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)

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