Mustakbil Scanning Report

Generated with ZAP on Tue 20 Dec 2022, at 17:14:31

Contents

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- https://www.mustakbil.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%)	4 (23.5%)	1 (5.9%)	1 (5.9%)	6 (35.3%)
	Low	0 (0.0%)	1 (5.9%)	5 (29.4%)	1 (5.9%)	7 (41.2%)
	Informational	0 (0.0%)	0 (0.0%)	2 (11.8%)	2 (11.8%)	4 (23.5%)
	Total	0 (0.0%)	5 (29.4%)	8 (47.1%)	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.mustakbil.com	0 (0)	6 (6)	7 (13)	4 (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
Absence of Anti-CSRF Tokens	Medium	2692 (15,835.3%)
CSP: Wildcard Directive	Medium	5734 (33,729.4%)
CSP: script-src unsafe-inline	Medium	5734 (33,729.4%)
CSP: style-src unsafe-inline	Medium	5733 (33,723.5%)
Total		17

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	1 (5.9%)
Cross-Domain Misconfiguration	Medium	2 (11.8%)
Cookie No HttpOnly Flag	Low	1 (5.9%)
Cookie Without Secure Flag	Low	1 (5.9%)
Cookie without SameSite Attribute	Low	1 (5.9%)
Cross-Domain JavaScript Source File Inclusion	Low	16796 (98,800.0%)
Information Disclosure - Debug Error Messages	Low	2 (11.8%)
Strict-Transport-Security Header Not Set	Low	5 (29.4%)
Timestamp Disclosure - Unix	Low	75 (441.2%)
Information Disclosure - Suspicious Comments	Informational	245 (1,441.2%)
Modern Web Application	Informational	5598 (32,929.4%)
Re-examine Cache-control Directives	Informational	5613 (33,017.6%)
Total		17

Alert type	Risk	Count
Retrieved from Cache	Informational	510 (3,000.0%)
Total		17

Alerts

Risk=Medium, Confidence=High (4)

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

CSP: Wildcard Directive (1)

▶ GET https://www.mustakbil.com/

CSP: script-src unsafe-inline (1)

▶ GET https://www.mustakbil.com/

CSP: style-src unsafe-inline (1)

▶ GET https://www.mustakbil.com/

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

▶ GET https://www.mustakbil.com/cdn-cgi/l/email-protection

Risk=Medium, Confidence=Medium (1)

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

Cross-Domain Misconfiguration (1)

▶ GET https://www.mustakbil.com/runtime.97f8e0ac640dce9c.js

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.mustakbil.com/

Risk=Low, Confidence=High (1)

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

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.mustakbil.com/cdn-cgi/l/email-protection

Risk=Low, Confidence=Medium (5)

https://www.mustakbil.com (5)

Cookie No HttpOnly Flag (1)

▶ GET https://www.mustakbil.com/sitemap.xml

Cookie Without Secure Flag (1)

▶ GET https://www.mustakbil.com/sitemap.xml

Cookie without SameSite Attribute (1)

▶ GET https://www.mustakbil.com/sitemap.xml

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.mustakbil.com/

Information Disclosure - Debug Error Messages (1)

▶ GET https://www.mustakbil.com/jobs/pakistan/lahore/copywriter

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.mustakbil.com/companies/pakistan/information-technology-and-services

Risk=Informational, Confidence=Medium (2)

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

Modern Web Application (1)

▶ GET https://www.mustakbil.com/

Retrieved from Cache (1)

▶ GET https://www.mustakbil.com/

Risk=Informational, Confidence=Low (2)

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

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.mustakbil.com/account/jobseeker

Re-examine Cache-control Directives (1)

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

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

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/fundamental

s/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/

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

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

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/

Retrieved from Cache

Source	raised by a passive scanner (Retrieved from Cache)
Reference	▪ https://tools.ietf.org/html/rfc7234 ▪ https://tools.ietf.org/html/rfc7231 ▪ http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)