AlFatah-Scan-Report

Generated with ZAP on Sun 18 Dec 2022, at 15:47:28

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.alfatah.pk

(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 (5.0%)	1 (5.0%)	0 (0.0%)	2 (10.0%)
	Medium	0 (0.0%)	3 (15.0%)	1 (5.0%)	1 (5.0%)	5 (25.0%)
	Low	0 (0.0%)	2 (10.0%)	3 (15.0%)	1 (5.0%)	6 (30.0%)
	Informational	0 (0.0%)	1 (5.0%)	2 (10.0%)	4 (20.0%)	7 (35.0%)
	Total	0 (0.0%)	7 (35.0%)	7 (35.0%)	6 (30.0%)	20 (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.alfatah.pk	2 (2)	5 (7)	6 (13)	7 (20)

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	2 (10.0%)
PII Disclosure	High	819 (4,095.0%)
Total		20

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	52500 (262,500.0%)
CSP: Wildcard Directive	Medium	733 (3,665.0%)
CSP: script-src unsafe-inline	Medium	733 (3,665.0%)
CSP: style-src unsafe-inline	Medium	733 (3,665.0%)
Cross-Domain Misconfiguration	Medium	185 (925.0%)
CSP: Notices	Low	48 (240.0%)
Cookie No HttpOnly Flag	Low	3385 (16,925.0%)
Cookie Without Secure Flag	Low	3398 (16,990.0%)
Cross-Domain JavaScript Source File Inclusion	Low	13135 (65,675.0%)
Strict-Transport-Security Header Not Set	Low	1 (5.0%)
Timestamp Disclosure - Unix	Low	49591 (247,955.0%)
Content Security Policy (CSP) Report-Only Header Found	Informational	2 (10.0%)
Total		20

Alert type	Risk	Count
Information Disclosure - Suspicious Comments	Informational	2735 (13,675.0%)
Loosely Scoped Cookie	Informational	692 (3,460.0%)
Modern Web Application	Informational	674 (3,370.0%)
Re-examine Cache-control Directives	Informational	611 (3,055.0%)
Retrieved from Cache	Informational	68 (340.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	204 (1,020.0%)
Total		20

Alerts

Risk=High, Confidence=High (1)

https://www.alfatah.pk (1)

PII Disclosure (1)

▶ GET https://www.alfatah.pk/cart

Risk=High, Confidence=Medium (1)

https://www.alfatah.pk (1)

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

▶ GET https://www.alfatah.pk/pages/grocery

Risk=Medium, Confidence=High (3)

https://www.alfatah.pk (3)

CSP: Wildcard Directive (1)

▶ GET https://www.alfatah.pk/admin

CSP: script-src unsafe-inline (1)

▶ GET https://www.alfatah.pk/admin

CSP: style-src unsafe-inline (1)

▶ GET https://www.alfatah.pk/admin

Risk=Medium, Confidence=Medium (1)

https://www.alfatah.pk (1)

Cross-Domain Misconfiguration (1)

▶ GET https://www.alfatah.pk/products/mk-bag-38socv8s3v-admiral-ir

Risk=Medium, Confidence=Low (1)

https://www.alfatah.pk (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.alfatah.pk/

Risk=Low, Confidence=High (2)

https://www.alfatah.pk (2)

CSP: Notices (1)

▶ GET https://www.alfatah.pk/admin

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.alfatah.pk/.well-known/shopify/monorail

Risk=Low, Confidence=Medium (3)

https://www.alfatah.pk (3)

Cookie No HttpOnly Flag (1)

▶ GET https://www.alfatah.pk/robots.txt

Cookie Without Secure Flag (1)

▶ GET https://www.alfatah.pk/robots.txt

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.alfatah.pk/

Risk=Low, Confidence=Low (1)

https://www.alfatah.pk (1)

Timestamp Disclosure - Unix (1)

▶ GET https://www.alfatah.pk/cart

Risk=Informational, Confidence=High (1)

https://www.alfatah.pk (1)

Content Security Policy (CSP) Report-Only Header Found (1)

▶ GET https://www.alfatah.pk/cart

Risk=Informational, Confidence=Medium (2)

https://www.alfatah.pk (2)

Modern Web Application (1)

▶ GET https://www.alfatah.pk/

Retrieved from Cache (1)

▶ GET https://www.alfatah.pk/52223574165/checkouts

Risk=Informational, Confidence=Low (4)

https://www.alfatah.pk (4)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.alfatah.pk/

Loosely Scoped Cookie (1)

▶ GET https://www.alfatah.pk/robots.txt

Re-examine Cache-control Directives (1)

▶ GET https://www.alfatah.pk/robots.txt

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

▶ GET https://www.alfatah.pk/collections/electronics?sort_by=created-descending

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

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

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

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

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

Content Security Policy (CSP) Report-Only Header Found

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	https://www.w3.org/TR/CSP2/ https://w3c.github.io/webappsec-csp/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/

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/

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)

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