Rozee.pk-Scan-Report

Generated with ZAP on Tue 20 Dec 2022, at 00:32:55

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.rozee.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%)	0 (0.0%)	0 (0.0%)	1 (5.0%)
	Medium	0 (0.0%)	1 (5.0%)	1 (5.0%)	1 (5.0%)	3 (15.0%)
	Low	0 (0.0%)	1 (5.0%)	8 (40.0%)	1 (5.0%)	10 (50.0%)
	Informational	0 (0.0%)	0 (0.0%)	2 (10.0%)	4 (20.0%)	6 (30.0%)
	Total	0 (0.0%)	3 (15.0%)	11 (55.0%)	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.rozee.pk	1 (1)	3 (4)	10 (14)	6 (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
PII Disclosure	High	55 (275.0%)
Absence of Anti-CSRF Tokens	Medium	8605 (43,025.0%)
Content Security Policy (CSP) Header Not Set	Medium	2012 (10,060.0%)
Missing Anti-clickjacking Header	Medium	32 (160.0%)
Total		20

Alert type	Risk	Count
Application Error Disclosure	Low	4 (20.0%)
Cookie No HttpOnly Flag	Low	19832 (99,160.0%)
Cookie Without Secure Flag	Low	9916 (49,580.0%)
Cookie with SameSite Attribute None	Low	9916 (49,580.0%)
Cookie without SameSite Attribute	Low	9929 (49,645.0%)
Cross-Domain JavaScript Source File Inclusion	Low	56712 (283,560.0%)
Private IP Disclosure	Low	1973 (9,865.0%)
Strict-Transport-Security Header Not Set	Low	3 (15.0%)
Timestamp Disclosure - Unix	Low	511 (2,555.0%)
X-Content-Type-Options Header Missing	Low	2061 (10,305.0%)
Charset Mismatch	Informational	1 (5.0%)
Information Disclosure - Suspicious Comments	Informational	6578 (32,890.0%)
Total		20

Alert type	Risk	Count
Loosely Scoped Cookie	Informational	16 (80.0%)
Modern Web Application	Informational	2007 (10,035.0%)
Re-examine Cache-control Directives	Informational	42 (210.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	224 (1,120.0%)
Total		20

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

▶ GET https://www.rozee.pk/UR/jobs-in-dera-ghazi-khan

Risk=Medium, Confidence=High (1)

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

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

▶ GET https://www.rozee.pk/

Risk=Medium, Confidence=Medium (1)

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

Missing Anti-clickjacking Header (1)

▶ GET https://www.rozee.pk/blog/

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.rozee.pk/

Risk=Low, Confidence=High (1)

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

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.rozee.pk/cdn-cgi/l/email-protection

Risk=Low, Confidence=Medium (8)

https://www.rozee.pk (8)

Application Error Disclosure (1)

▶ GET https://www.rozee.pk/beta45/

Cookie No HttpOnly Flag (1)

▶ GET https://www.rozee.pk/robots.txt

Cookie Without Secure Flag (1)

▶ GET https://www.rozee.pk/sitemap.xml

Cookie with SameSite Attribute None (1)

▶ GET https://www.rozee.pk/sitemap.xml

Cookie without SameSite Attribute (1)

▶ GET https://www.rozee.pk/sitemap.xml

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.rozee.pk/

Private IP Disclosure (1)

▶ GET https://www.rozee.pk/

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

▶ GET https://www.rozee.pk/robots.txt

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.rozee.pk/blog/

Risk=Informational, Confidence=Medium (2)

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

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.rozee.pk/

Modern Web Application (1)

▶ GET https://www.rozee.pk/

Risk=Informational, Confidence=Low (4)

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

Charset Mismatch (1)

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

Loosely Scoped Cookie (1)

▶ GET https://www.rozee.pk/UR/?chlng=y

Re-examine Cache-control Directives (1)

▶ GET https://www.rozee.pk/robots.txt

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

▶ GET https://www.rozee.pk/site/error?e=cnf_sitemap.xml

Appendix

Alert types

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

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

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

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)

CWE ID	200
WASC ID	13

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 with SameSite Attribute None

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

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

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

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

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

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