LinkedIn.com Scanning Report

Generated with ZAP on Mon 19 Dec 2022, at 21:22:30

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://pk.linkedin.com
- https://pk.linkedin.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 (19.0%)	0 (0.0%)	1 (4.8%)	5 (23.8%)
	Low	0 (0.0%)	3 (14.3%)	5 (23.8%)	1 (4.8%)	9 (42.9%)
	Informational	0 (0.0%)	0 (0.0%)	3 (14.3%)	4 (19.0%)	7 (33.3%)
	Total	0 (0.0%)	7 (33.3%)	8 (38.1%)	6 (28.6%)	21 (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://pk.linkedin.com	0 (0)	5 (5)	9 (14)	7 (21)

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	7292 (34,723.8%)
CSP: Wildcard Directive	Medium	1089 (5,185.7%)
CSP: script-src unsafe-inline	Medium	123 (585.7%)
CSP: style-src unsafe-inline	Medium	1089 (5,185.7%)
Content Security Policy (CSP) Header Not Set	Medium	2218 (10,561.9%)
Total		21

Alert type	Risk	Count
CSP: Notices	Low	1027 (4,890.5%)
Cookie No HttpOnly Flag	Low	6875 (32,738.1%)
Cookie Without Secure Flag	Low	6606 (31,457.1%)
Cookie with SameSite Attribute None	Low	269 (1,281.0%)
Cookie without SameSite Attribute	Low	6763 (32,204.8%)
Cross-Domain JavaScript Source File Inclusion	Low	2055 (9,785.7%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1 (4.8%)
Strict-Transport-Security Header Not Set	Low	2228 (10,609.5%)
Timestamp Disclosure - Unix	Low	594 (2,828.6%)
Content-Type Header Missing	Informational	1 (4.8%)
Information Disclosure - Sensitive Information in URL	Informational	31 (147.6%)
Information Disclosure - Suspicious Comments	Informational	3426 (16,314.3%)
Total		21

Alert type	Risk	Count
Loosely Scoped Cookie	Informational	2453 (11,681.0%)
Modern Web Application	Informational	3188 (15,181.0%)
Re-examine Cache-control Directives	Informational	990 (4,714.3%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	3178 (15,133.3%)
Total		21

Alerts

Risk=Medium, Confidence=High (4)

https://pk.linkedin.com (4)

CSP: Wildcard Directive (1)

▶ GET https://pk.linkedin.com

CSP: script-src unsafe-inline (1)

▶ GET https://pk.linkedin.com/sitemap.xml

CSP: style-src unsafe-inline (1)

▶ GET https://pk.linkedin.com

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

▶ GET https://pk.linkedin.com/pub/dir/+/+?trk=homepage-basic

Risk=Medium, Confidence=Low (1)

https://pk.linkedin.com (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://pk.linkedin.com

Risk=Low, Confidence=High (3)

https://pk.linkedin.com (3)

CSP: Notices (1)

▶ GET https://pk.linkedin.com

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▶ GET https://pk.linkedin.com/csp/

Strict-Transport-Security Header Not Set (1)

▶ GET https://pk.linkedin.com/pub/dir/+/+?trk=homepage-basic

Risk=Low, Confidence=Medium (5)

https://pk.linkedin.com (5)

Cookie No HttpOnly Flag (1)

▶ GET https://pk.linkedin.com/robots.txt

Cookie Without Secure Flag (1)

▶ GET https://pk.linkedin.com/authwall

Cookie with SameSite Attribute None (1)

▶ GET https://pk.linkedin.com/robots.txt

Cookie without SameSite Attribute (1)

▶ GET https://pk.linkedin.com/authwall

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://pk.linkedin.com

Risk=Low, Confidence=Low (1)

https://pk.linkedin.com (1)

Timestamp Disclosure - Unix (1)

▶ GET https://pk.linkedin.com

Risk=Informational, Confidence=Medium (3)

https://pk.linkedin.com (3)

Content-Type Header Missing (1)

▶ GET https://pk.linkedin.com/fizzy/admin

Information Disclosure - Sensitive Information in URL (1)

▶ GET https://pk.linkedin.com/jobs/engineering-jobs-islamabad?emailAddress=foo-

bar%40example.com&jserpUrl=https%3A%2F%2Fpk.linkedin.com%2Fjobs%2Fengineering-jobs-islamabad%3Ftrk%3Dhomepage-basic_suggested-search&keywords=Engineering&pageType=JSERP&trk=homepage-basic_suggested-search

Modern Web Application (1)

▶ GET https://pk.linkedin.com/learning/search

Risk=Informational, Confidence=Low (4)

https://pk.linkedin.com (4)

Information Disclosure - Suspicious Comments (1)

▶ GET https://pk.linkedin.com/sitemap.xml

Loosely Scoped Cookie (1)

▶ GET https://pk.linkedin.com/robots.txt

Re-examine Cache-control Directives (1)

▶ GET https://pk.linkedin.com/robots.txt

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

▶ GET https://pk.linkedin.com/?trk=guest_homepage-basic_nav-header-logo

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/fundamental

s/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

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/

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 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

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200
WASC ID	13
Reference	▪ http://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 ▪ 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

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-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 - Sensitive Information in URL

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	200
WASC ID	13

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