OLX-ZAP Scanning Report

Generated with ZAP on Sun 18 Dec 2022, at 16:04:24

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://www.olx.com.pk
- https://safebrowsing.googleapis.com
- https://play.google.com
- https://sdk-01.moengage.com
- https://tags.bluekai.com
- https://www.googletagservices.com
- https://tpc.googlesyndication.com
- https://partner.googleadservices.com
- https://963781534ec0cefa5be922c6d5998500.safeframe.googlesyndication.com
- https://www.facebook.com
- https://googleads.g.doubleclick.net
- https://stats.g.doubleclick.net
- https://fonts.gstatic.com
- https://adservice.google.com
- https://adservice.google.com.pk
- https://analytics.google.com
- https://pagead2.googlesyndication.com
- https://www.google-analytics.com
- https://connect.facebook.net

- https://cdn.moengage.com
- https://securepubads.g.doubleclick.net
- https://www.googletagmanager.com
- https://accounts.google.com
- https://ovation.olx.com.pk
- https://search-strat-production-olx-pk-3pgjxaluaukyelqkf2cnvftrwq.ap-southeast-1.es.amazonaws.com
- https://www.olx.com.pk
- https://olx.com.pk
- https://incoming.telemetry.mozilla.org
- http://olx.pk
- https://www.google.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%)	1 (3.6%)	1 (3.6%)	0 (0.0%)	2 (7.1%)
	Medium	0 (0.0%)	5 (17.9%)	4 (14.3%)	0 (0.0%)	9 (32.1%)
	Low	0 (0.0%)	4 (14.3%)	6 (21.4%)	1 (3.6%)	11 (39.3%)
	Informational	0 (0.0%)	0 (0.0%)	3 (10.7%)	3 (10.7%)	6 (21.4%)
	Total	0 (0.0%)	10 (35.7%)	14 (50.0%)	4 (14.3%)	28 (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)

	Risk			
Site	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://play.google.com	0 (0)	0 (0)	0 (0)	1 (1)
https://tags.bluekai.com	1 (1)	0 (1)	0 (1)	0 (1)
https://analytics.google.com	0 (0)	1 (1)	0 (1)	0 (1)
https://accounts.google.com	0 (0)	1 (1)	1 (2)	0 (2)
https://ovation.olx.com.pk	0 (0)	1 (1)	0 (1)	0 (1)
https://search-strat-production-olx-pk-3pgjxaluaukyelqkf2cnvftrwq.ap-southeast-1.es.amazonaws.com	0 (0)	1 (1)	0 (1)	0 (1)
https://www.olx.com.pk	1 (1)	5 (6)	7 (13)	4 (17)
https://olx.com.pk	0 (0)	0 (0)	2 (2)	1 (3)
https://www.google.com	0 (0)	0 (0)	1 (1)	0 (1)

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
Open Redirect	High	1 (3.6%)
PII Disclosure	High	471 (1,682.1%)
Application Error Disclosure	Medium	2 (7.1%)
CSP: Wildcard Directive	Medium	203 (725.0%)
CSP: script-src unsafe-inline	Medium	201 (717.9%)
CSP: style-src unsafe-inline	Medium	202 (721.4%)
Content Security Policy (CSP) Header Not Set	Medium	24 (85.7%)
Cross-Domain Misconfiguration	Medium	24 (85.7%)
Missing Anti-clickjacking Header	Medium	18 (64.3%)
Session ID in URL Rewrite	Medium	1 (3.6%)
Vulnerable JS Library	Medium	1 (3.6%)
Total		28

Alert type	Risk	Count
CSP: Notices	Low	3 (10.7%)
Cookie No HttpOnly Flag	Low	6 (21.4%)
Cookie with SameSite Attribute None	Low	15 (53.6%)
Cookie without SameSite Attribute	Low	3 (10.7%)
Cross-Domain JavaScript Source File Inclusion	Low	11 (39.3%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	11 (39.3%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	11 (39.3%)
Strict-Transport-Security Header Not Set	Low	107 (382.1%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	2 (7.1%)
Timestamp Disclosure - Unix	Low	5767 (20,596.4%)
X-Content-Type-Options Header Missing	Low	242 (864.3%)
Information Disclosure - Sensitive Information in URL	Informational	2 (7.1%)
Total		28

Alert type	Risk	Count
Information Disclosure - Suspicious Comments	Informational	391 (1,396.4%)
Loosely Scoped Cookie	Informational	16 (57.1%)
Modern Web Application	Informational	184 (657.1%)
Re-examine Cache-control Directives	Informational	191 (682.1%)
Retrieved from Cache	Informational	49 (175.0%)
Total		28

Alerts

Risk=High, Confidence=High (1)

https://www.olx.com.pk (1)

PII Disclosure (1)

▶ GET https://www.olx.com.pk/

Risk=High, Confidence=Medium (1)

https://tags.bluekai.com (1)

Open Redirect (1)

```
▶ GET https://tags.bluekai.com/site/82519?
limit=0&phint=event%3Dimp&phint=aid%3D5481501&phint=cid%3D27151701&
phint=crid%3D181831216&phint=pid%3D352225071&phint=segment%3DINMK-
AUSTRALI&redir=https%3A%2F%2Fads.travelaudience.com%2Ftrg.gif%3Fds%
3Ddp%26acc%3DSC%26lvl%3D1%26pl%3Ddubai%26pt%3D16%26rcm=413%26pix%3D
0%26exid%3D$_BK_UUID%26dp%3Devent_type%3Aimpression
```

Risk=Medium, Confidence=High (5)

https://analytics.google.com (1)

Session ID in URL Rewrite (1)

```
▶ POST https://analytics.google.com/g/collect?v=2&tid=G-
YP1ZBNYRVD&gtm=2oebu0&_p=1168057046&_gaz=1&ul=en&cid=1296513226.167
0942622&sr=1366x768&_s=1&sid=1670942622&sct=1&seg=0&dl=https%3A%2F%
2Fwww.olx.com.pk%2F&dt=OLX%20-
%20Buy%20and%20Sell%20for%20free%20anywhere%20in%20Pakistan%20with%
20OLX%20online%20classifieds&en=page_view&_fv=1&_nsi=1&_ss=2&ep.web
site_section=main_site&ep.page_type=home&epn.page_number=1&epn.loc_
id=1000001&ep.loc_name=Pakistan&ep.loc_breadcrumb=%3B1000001%3B&ep.
loc_1_name=&ep.loc_1_id=&ep.loc_2_name=&ep.loc_2_id=&ep.loc_3_name=
&ep.loc_3_id=&ep.area_unit=Sq.%20M.&ep.fresh_recommendations=106136
9662%2C1062615641%2C1060944496%2C1062598386%2C1061246849%2C10626156
34%2C1060265737%2C1062367774%2C1059066621%2C1062615632%2C1062377137
%2C1061359377%2C1062615630%2C1010027605%2C1062615628%2C1062615625%2
C1062615624%2C1062547733%2C1062324312%2C1062225473&ep.popular_categ
ories=1453%2C84%2C81%2C1721%2C729%2C1455%2C40
```

https://ovation.olx.com.pk (1)

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

```
▶ OPTIONS https://ovation.olx.com.pk/ingest/adMetric/
```

https://www.olx.com.pk (3)

CSP: Wildcard Directive (1)

▶ GET https://www.olx.com.pk/

CSP: script-src unsafe-inline (1)

▶ GET https://www.olx.com.pk/

CSP: style-src unsafe-inline (1)

▶ GET https://www.olx.com.pk/

Risk=Medium, Confidence=Medium (4)

https://accounts.google.com (1)

Missing Anti-clickjacking Header (1)

▶ GET https://accounts.google.com/gsi/iframe/select?client_id=874470485231-c7l7qahib20c03gpab475f1j0una1pcu.apps.googleusercontent.com&ux_mode=popup&ui_mode=card&as=NHK%2FCnNmfszOJNsC7SO7PA&is_itp=true&channel_id=0f7685ee17e6afe366c13ef75a50e16d9c05d71f6a17c303c09aea685a36a85f&origin=https%3A%2F%2Fwww.olx.com.pk

https://search-strat-production-olx-pk-3pgjxaluaukyelqkf2cnvftrwq.ap-southeast-1.es.amazonaws.com (1)

Cross-Domain Misconfiguration (1)

▶ OPTIONS https://search-strat-production-olx-pk-3pgjxaluaukyelqkf2cnvftrwq.ap-southeast-1.es.amazonaws.com/_msearch?

filter_path=took%2C*.took%2C*.suggest.*.options.text%2C*.suggest.*.options._source.*%2C*.hits.total.*%2C*.hits.hits._source.*%2C*.hits.hits._score%2C*.hits.hits.highlight.*%2C*.error%2C*.aggregations.*.buckets.key%2C*.aggregations.*.buckets.doc_count%2C*.aggregations.*.buckets.complex_value.hits.hits._source%2C*.aggregations.*.filtered_agg.facet.buckets.key%2C*.aggregations.*.filtered_agg.facet.buckets.doc_count%2C*.aggregations.*.filtered_agg.facet.buckets.complex_value.hits.hits._source

https://www.olx.com.pk (2)

Application Error Disclosure (1)

▶ GET https://www.olx.com.pk/assets/main.desktop.7ab20b473c6fe1526d97.js

Vulnerable JS Library (1)

▶ GET https://www.olx.com.pk/motors/_next/static/chunks/main-211badacbe468caafeb8.js

Risk=Low, Confidence=High (4)

https://accounts.google.com (1)

CSP: Notices (1)

▶ GET https://accounts.google.com/gsi/iframe/select?client_id=874470485231-c7l7qahib20c03gpab475f1j0una1pcu.apps.googleusercontent.com&ux_mode=popup&ui_mode=card&as=NHK%2FCnNmfszOJNsC7SO7PA&is_itp=true&channel_id=0f7685ee17e6afe366c13ef75a50e16d9c05d71f6a17c303c09aea685a36a85f&origin=https%3A%2F%2Fwww.olx.com.pk

https://www.olx.com.pk (1)

Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec) (1)

▶ GET https://www.olx.com.pk/api/banners?platform=web

https://olx.com.pk (2)

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

▶ GET https://olx.com.pk/

Strict-Transport-Security Header Not Set (1)

▶ GET https://olx.com.pk/

Risk=Low, Confidence=Medium (6)

https://www.olx.com.pk (5)

Cookie No HttpOnly Flag (1)

▶ GET https://www.olx.com.pk/

Cookie with SameSite Attribute None (1)

▶ GET https://www.olx.com.pk/

Cookie without SameSite Attribute (1)

▶ GET https://www.olx.com.pk/

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.olx.com.pk/motors/

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

▶ GET https://www.olx.com.pk/motors/

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

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

▶ GET https://www.google.com/complete/search?client=firefox&q=olx

Risk=Low, Confidence=Low (1)

https://www.olx.com.pk (1)

Timestamp Disclosure - Unix (1)

▶ GET https://www.olx.com.pk/

Risk=Informational, Confidence=Medium (3)

https://play.google.com (1)

Information Disclosure - Sensitive Information in URL (1)

▶ OPTIONS https://play.google.com/log?format=json&hasfast=true&authuser=0

https://www.olx.com.pk (1)

Modern Web Application (1)

▶ GET https://www.olx.com.pk/

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

Retrieved from Cache (1)

▶ GET https://olx.com.pk/

Risk=Informational, Confidence=Low (3)

https://www.olx.com.pk (3)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.olx.com.pk/

Loosely Scoped Cookie (1)

▶ GET https://www.olx.com.pk/

Re-examine Cache-control Directives (1)

▶ GET https://www.olx.com.pk/

Appendix

Alert types

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

Open Redirect

Source	raised by a passive scanner (Open Redirect)
CWE ID	601
WASC ID	38
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html ▪ https://cwe.mitre.org/data/definitions/601.html

PII Disclosure

Source	raised by a passive scanner (PII Disclosure)
CWE ID	359
WASC ID	13

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

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

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

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

Session ID in URL Rewrite

Source	raised by a passive scanner (Session ID in URL Rewrite)
CWE ID	200
WASC ID	13
Reference	- http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	- https://github.com/vercel/next.js/security/advisories/GHSA-fmvm-x8mv-47mj

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 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 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

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

Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	▪ http://tools.ietf.org/html/rfc6797#section-8.1

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

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/

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)