

AliExpress Scanning Report

Generated with  ZAP on Mon 19 Dec 2022, at 18:32:55

Contents

- [About this report](#)
 - [Report parameters](#)
- [Summaries](#)
 - [Alert counts by risk and confidence](#)
 - [Alert counts by site and risk](#)
 - [Alert counts by alert type](#)
- [Alerts](#)
 - [Risk=High, Confidence=High \(1\)](#)
 - [Risk=Medium, Confidence=High \(1\)](#)
 - [Risk=Medium, Confidence=Medium \(1\)](#)
 - [Risk=Medium, Confidence=Low \(1\)](#)
 - [Risk=Low, Confidence=High \(3\)](#)
 - [Risk=Low, Confidence=Medium \(5\)](#)

- [Risk=Low, Confidence=Low \(1\)](#)
- [Risk=Informational, Confidence=Medium \(1\)](#)
- [Risk=Informational, Confidence=Low \(3\)](#)
- [Appendix](#)
 - [Alert types](#)

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.aliexpress.com>
- <https://www.aliexpress.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				Total
	User Confirmed	High	Medium	Low	
Risk	High	0 (0.0%)	1 (5.9%)	0 (0.0%)	1 (5.9%)
	Medium	0 (0.0%)	1 (5.9%)	1 (5.9%)	3 (17.6%)
	Low	0 (0.0%)	3 (17.6%)	5 (29.4%)	9 (52.9%)
	Informational	0 (0.0%)	0 (0.0%)	1 (5.9%)	3 (17.6%)
	1	0 (0.0%)	0 (0.0%)	1 (5.9%)	4 (23.5%)
	Total	0 (0.0%)	5 (29.4%)	7 (41.2%)	5 (29.4%)
					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.)

Site	Risk			Informational
	High (= High)	Medium (>= Medium)	Low (>= Low)	(>= Informational)
https://www.aliexpress.com	1 (1)	3 (4)	9 (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
PII Disclosure	High	110 (647.1%)
Absence of Anti-CSRF Tokens	Medium	172 (1,011.8%)
Content Security Policy (CSP) Header Not Set	Medium	179 (1,052.9%)
Total		17

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	172 (1,011.8%)
Cookie No HttpOnly Flag	Low	552 (3,247.1%)
Cookie Without Secure Flag	Low	742 (4,364.7%)
Cookie without SameSite Attribute	Low	742 (4,364.7%)
Cross-Domain JavaScript Source File Inclusion	Low	855 (5,029.4%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	3 (17.6%)
Strict-Transport-Security Header Not Set	Low	5 (29.4%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	8 (47.1%)
Timestamp Disclosure - Unix	Low	226 (1,329.4%)
X-Content-Type-Options Header Missing	Low	173 (1,017.6%)
Information Disclosure - Suspicious Comments	Informational	332 (1,952.9%)
Loosely Scoped Cookie	Informational	182 (1,070.6%)
Total		17

Alert type	Risk	Count
Modern Web Application	Informational	4 (23.5%)
Re-examine Cache-control Directives	Informational	174 (1,023.5%)
Total		17

Alerts

Risk=High, Confidence=High (1)

<https://www.aliexpress.com> (1)

[PII Disclosure](#) (1)

► GET https://www.aliexpress.com/api/data_homepage.do

Risk=Medium, Confidence=High (1)

<https://www.aliexpress.com> (1)

[Content Security Policy \(CSP\) Header Not Set](#) (1)

► GET <https://www.aliexpress.com/>

Risk=Medium, Confidence=Medium (1)

<https://www.aliexpress.com> (1)

Missing Anti-clickjacking Header (1)

► GET <https://www.aliexpress.com/store/all-wholesale-products/>

Risk=Medium, Confidence=Low (1)

<https://www.aliexpress.com> (1)

Absence of Anti-CSRF Tokens (1)

► GET <https://www.aliexpress.com/>

Risk=Low, Confidence=High (3)

<https://www.aliexpress.com> (3)

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

► GET [https://www.aliexpress.com/detail/*Ajax.do\\$](https://www.aliexpress.com/detail/*Ajax.do$)

Strict-Transport-Security Header Not Set (1)

► GET <https://www.aliexpress.com/search/>

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

► GET <https://www.aliexpress.com/robots.txt>

Risk=Low, Confidence=Medium (5)

<https://www.aliexpress.com> (5)

Cookie No HttpOnly Flag (1)

► GET https://www.aliexpress.com/

Cookie Without Secure Flag (1)

► GET https://www.aliexpress.com/

Cookie without SameSite Attribute (1)

► GET https://www.aliexpress.com/

Cross-Domain JavaScript Source File Inclusion (1)

► GET https://www.aliexpress.com/

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

► GET https://www.aliexpress.com/store/all-wholesale-products/

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

► GET https://www.aliexpress.com/

Risk=Informational, Confidence=Medium (1)

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

Modern Web Application (1)

► GET https://www.aliexpress.com/search/

Risk=Informational, Confidence=Low (3)

<https://www.aliexpress.com> (3)

Information Disclosure - Suspicious Comments (1)

► GET <https://www.aliexpress.com/>

Loosely Scoped Cookie (1)

► GET <https://www.aliexpress.com/>

Re-examine Cache-control Directives (1)

► GET <https://www.aliexpress.com/>

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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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

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

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 - 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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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/