Walmart-Scan-Report

Generated with ZAP on Fri 2 Dec 2022, at 19:08:09

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.walmart.com`
- `https://www.walmart.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%)	3 (14.3%)	2 (9.5%)	1 (4.8%)	6 (28.6%)
	Low	0 (0.0%)	2 (9.5%)	6 (28.6%)	1 (4.8%)	9 (42.9%)
	Informational	0 (0.0%)	1 (4.8%)	2 (9.5%)	3 (14.3%)	6 (28.6%)
	Total	0 (0.0%)	6 (28.6%)	10 (47.6%)	5 (23.8%)	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://www.walmart.com	0 (0)	6 (6)	9 (15)	6 (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	47 (223.8%)
CSP: Wildcard Directive	Medium	18 (85.7%)
CSP: style-src unsafe-inline	Medium	18 (85.7%)
Content Security Policy (CSP) Header Not Set	Medium	819 (3,900.0%)
Total		21

Alert type	Risk	Count
Cross-Domain Misconfiguration	Medium	1 (4.8%)
Missing Anti-clickjacking Header	Medium	783 (3,728.6%)
CSP: Notices	Low	18 (85.7%)
Cookie No HttpOnly Flag	Low	4490 (21,381.0%)
Cookie Without Secure Flag	Low	4484 (21,352.4%)
Cookie with SameSite Attribute None	Low	1288 (6,133.3%)
Cookie without SameSite Attribute	Low	4484 (21,352.4%)
Cross-Domain JavaScript Source File Inclusion	Low	616 (2,933.3%)
Strict-Transport-Security Header Not Set	Low	851 (4,052.4%)
Timestamp Disclosure - Unix	Low	2713 (12,919.0%)
X-Content-Type-Options Header Missing	Low	836 (3,981.0%)
Content Security Policy (CSP) Report-Only Header Found	Informational	18 (85.7%)
Total		21

Alert type	Risk	Count
Content-Type Header Missing	Informational	11 (52.4%)
Information Disclosure - Suspicious Comments	Informational	55 (261.9%)
Loosely Scoped Cookie	Informational	47 (223.8%)
Modern Web Application	Informational	48 (228.6%)
Re-examine Cache-control Directives	Informational	800 (3,809.5%)
Total		21

Alerts

Risk=Medium, Confidence=High (3)

https://www.walmart.com (3)

CSP: Wildcard Directive (1)

▶ GET https://www.walmart.com/

CSP: style-src unsafe-inline (1)

▶ GET https://www.walmart.com/

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

▶ GET https://www.walmart.com/0/

Risk=Medium, Confidence=Medium (2)

https://www.walmart.com (2)

Cross-Domain Misconfiguration (1)

▶ GET https://www.walmart.com/px/PXu6b0qd2S/init.js

Missing Anti-clickjacking Header (1)

▶ GET https://www.walmart.com/blocked?g=b&url=L3NpdGVtYXAueG1s&uuid=a4793b61-7248-11ed-9f08-5a584f6a524b&vid

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.walmart.com/

Risk=Low, Confidence=High (2)

https://www.walmart.com (2)

CSP: Notices (1)

▶ GET https://www.walmart.com/

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.walmart.com/0/

Risk=Low, Confidence=Medium (6)

https://www.walmart.com (6)

Cookie No HttpOnly Flag (1)

▶ GET https://www.walmart.com/sitemap.xml

Cookie Without Secure Flag (1)

▶ GET https://www.walmart.com/sitemap.xml

Cookie with SameSite Attribute None (1)

▶ GET https://www.walmart.com/

Cookie without SameSite Attribute (1)

▶ GET https://www.walmart.com/sitemap.xml

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.walmart.com/

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

▶ GET https://www.walmart.com/robots.txt

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.walmart.com/sitemap.xml

Risk=Informational, Confidence=High (1)

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

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

▶ GET https://www.walmart.com/

Risk=Informational, Confidence=Medium (2)

https://www.walmart.com (2)

Content-Type Header Missing (1)

▶ GET https://www.walmart.com/store/ajax/local-store

Modern Web Application (1)

▶ GET https://www.walmart.com/

Risk=Informational, Confidence=Low (3)

https://www.walmart.com (3)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.walmart.com/

Loosely Scoped Cookie (1)

▶ GET https://www.walmart.com/api/

Re-examine Cache-control Directives (1)

▶ GET https://www.walmart.com/robots.txt

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/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

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

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

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/

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 - 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/