LifeStyleStore-Scan-Report

Generated with ZAP on Mon 28 Nov 2022, at 17:56:18

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://localhost`

(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%)	2 (13.3%)	3 (20.0%)	1 (6.7%)	6 (40.0%)
	Low	0 (0.0%)	1 (6.7%)	5 (33.3%)	0 (0.0%)	6 (40.0%)
	Informational	0 (0.0%)	0 (0.0%)	1 (6.7%)	2 (13.3%)	3 (20.0%)
	Total	0 (0.0%)	3 (20.0%)	9 (60.0%)	3 (20.0%)	15 (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	http://localhost	0 (0)	6 (6)	6 (12)	3 (15)

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	3 (20.0%)
Application Error Disclosure	Medium	1 (6.7%)
Content Security Policy (CSP) Header Not Set	Medium	11 (73.3%)
Hidden File Found	Medium	2 (13.3%)
Missing Anti-clickjacking Header	Medium	9 (60.0%)
Total		15

Alert type	Risk	Count
Vulnerable JS Library	Medium	2 (13.3%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	2 (13.3%)
Cookie No HttpOnly Flag	Low	1 (6.7%)
Cookie without SameSite Attribute	Low	1 (6.7%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	11 (73.3%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	36 (240.0%)
X-Content-Type-Options Header Missing	Low	32 (213.3%)
Information Disclosure - Suspicious Comments	Informational	3 (20.0%)
Loosely Scoped Cookie	Informational	5 (33.3%)
Modern Web Application	Informational	4 (26.7%)
Total		15

Alerts

Risk=Medium, Confidence=High (2)

http://localhost (2)

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

▶ GET http://localhost/LifestyleStore/LifestyleStore/index.php

Hidden File Found (1)

▶ GET http://localhost/server-status

Risk=Medium, Confidence=Medium (3)

http://localhost (3)

Application Error Disclosure (1)

▶ POST http://localhost/LifestyleStore/LifestyleStore/setting_script.php

Missing Anti-clickjacking Header (1)

▶ GET http://localhost/LifestyleStore/LifestyleStore/index.php

Vulnerable JS Library (1)

▶ GET http://localhost/LifestyleStore/LifestyleStore/bootstrap/js/bootstrap.min.js

Risk=Medium, Confidence=Low (1)

http://localhost (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://localhost/LifestyleStore/LifestyleStore/login.php

Risk=Low, Confidence=High (1)

http://localhost (1)

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

▶ GET http://localhost/LifestyleStore/LifestyleStore/index.php

Risk=Low, Confidence=Medium (5)

http://localhost (5)

Big Redirect Detected (Potential Sensitive Information Leak) (1)

▶ GET http://localhost/LifestyleStore/LifestyleStore/success.php?id=5

Cookie No HttpOnly Flag (1)

▶ GET http://localhost/LifestyleStore/LifestyleStore/index.php

Cookie without SameSite Attribute (1)

▶ GET http://localhost/LifestyleStore/LifestyleStore/index.php

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

▶ GET http://localhost/LifestyleStore/LifestyleStore/index.php

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

▶ GET http://localhost/LifestyleStore/LifestyleStore/index.php

Risk=Informational, Confidence=Medium (1)

http://localhost (1)

Modern Web Application (1)

▶ GET http://localhost/LifestyleStore/LifestyleStore/bootstrap/js/jquery-3.2.1.min.js

Risk=Informational, Confidence=Low (2)

http://localhost (2)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost/LifestyleStore/LifestyleStore/bootstrap/js/jquery-3.2.1.min.js

Loosely Scoped Cookie (1)

▶ GET http://localhost/LifestyleStore/LifestyleStore/index.php

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

Application Error Disclosure

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

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/

Hidden File Found

Source	raised by an active scanner (Hidden File Finder)
CWE ID	538
WASC ID	13
Reference	▪ https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html ▪ https://httpd.apache.org/docs/current/mod/mod_status.html

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

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	▪ https://github.com/twbs/bootstrap/issues/28236 ▪ https://github.com/twbs/bootstrap/issues/20184 ▪ https://github.com/advisories/GHSA-4p24-vmcr-4gqj

Big Redirect Detected (Potential Sensitive Information Leak)

Source	raised by a passive scanner (Big Redirect Detected (Potential Sensitive Information Leak))
CWE ID	201
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 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

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

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	- 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)