EMS-Scan-Report

Generated with ZAP on Tue 20 Dec 2022, at 13:28:57

Contents

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- `https://localhost`
- `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%)	1 (4.2%)	6 (25.0%)	2 (8.3%)	9 (37.5%)
	Low	0 (0.0%)	2 (8.3%)	7 (29.2%)	0 (0.0%)	9 (37.5%)
	Informational	0 (0.0%)	0 (0.0%)	2 (8.3%)	4 (16.7%)	6 (25.0%)
	Total	0 (0.0%)	3 (12.5%)	15 (62.5%)	6 (25.0%)	24 (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://localhost	0 (0)	5 (5)	3 (8)	3 (11)
	http://localhost	0 (0)	4 (4)	6 (10)	3 (13)

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	9 (37.5%)
Application Error Disclosure	Medium	18 (75.0%)
Content Security Policy (CSP) Header Not Set	Medium	32 (133.3%)
Directory Browsing	Medium	15 (62.5%)
Total		24

Alert type	Risk	Count
Directory Browsing - Apache 2	Medium	18 (75.0%)
Missing Anti-clickjacking Header	Medium	27 (112.5%)
Parameter Tampering	Medium	2 (8.3%)
Secure Pages Include Mixed Content (Including Scripts)	Medium	4 (16.7%)
Vulnerable JS Library	Medium	2 (8.3%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	2 (8.3%)
Cookie No HttpOnly Flag	Low	2 (8.3%)
Cookie Without Secure Flag	Low	1 (4.2%)
Cookie without SameSite Attribute	Low	2 (8.3%)
Cross-Domain JavaScript Source File Inclusion	Low	10 (41.7%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	11 (45.8%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	64 (266.7%)
Total		24

Alert type	Risk	Count
Strict-Transport-Security Header Not Set	Low	45 (187.5%)
X-Content-Type-Options Header Missing	Low	55 (229.2%)
Information Disclosure - Suspicious Comments	Informational	16 (66.7%)
Loosely Scoped Cookie	Informational	3 (12.5%)
Modern Web Application	Informational	9 (37.5%)
Re-examine Cache-control Directives	Informational	18 (75.0%)
User Agent Fuzzer	Informational	216 (900.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	4 (16.7%)
Total		24

Alerts

Risk=Medium, Confidence=High (1)

http://localhost (1)

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

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/

Risk=Medium, Confidence=Medium (6)

https://localhost (4)

Application Error Disclosure (1)

▶ GET https://localhost/Employee%20Leave%20Management%20System/

Directory Browsing (1)

▶ GET https://localhost/Employee%20Leave%20Management%20System/

Directory Browsing - Apache 2 (1)

▶ GET https://localhost/Employee%20Leave%20Management%20System/

Secure Pages Include Mixed Content (Including Scripts) (1)

▶ GET
https://localhost/Employee%20Leave%20Management%20System/elms/

http://localhost (2)

Missing Anti-clickjacking Header (1)

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/

Vulnerable JS Library (1)

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/assets/plugins/jquery/jquery-2.2.0.min.js

Risk=Medium, Confidence=Low (2)

https://localhost (1)

Parameter Tampering (1)

▶ POST
https://localhost/Employee%20Leave%20Management%20System/elms/admin/

http://localhost (1)

Absence of Anti-CSRF Tokens (1)

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/

Risk=Low, Confidence=High (2)

https://localhost (1)

Strict-Transport-Security Header Not Set (1)

▶ GET
https://localhost/Employee%20Leave%20Management%20System/elms/

http://localhost (1)

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

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/assets/css/materialdesign.css

Risk=Low, Confidence=Medium (7)

https://localhost (2)

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

▶ GET https://localhost/Employee%20Leave%20Management%20System

Cookie Without Secure Flag (1)

▶ GET
https://localhost/Employee%20Leave%20Management%20System/elms/

http://localhost (5)

Cookie No HttpOnly Flag (1)

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/

Cookie without SameSite Attribute (1)

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/

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

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/

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

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/assets/css/materialdesign.css

Risk=Informational, Confidence=Medium (2)

https://localhost (1)

User Agent Fuzzer (1)

▶ GET https://localhost

http://localhost (1)

Modern Web Application (1)

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/

Risk=Informational, Confidence=Low (4)

https://localhost (2)

Re-examine Cache-control Directives (1)

▶ GET https://localhost/Employee%20Leave%20Management%20System/

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

▶ POST
https://localhost/Employee%20Leave%20Management%20System/elms/

http://localhost (2)

Information Disclosure - Suspicious Comments (1)

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/assets/plugins/jquery/jquery-2.2.0.min.js

Loosely Scoped Cookie (1)

▶ GET
http://localhost/Employee%20Leave%20Management%20System/elms/

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/

Directory Browsing

Source	raised by an active scanner (Directory Browsing)
CWE ID	548
WASC ID	48
Reference	http://httpd.apache.org/docs/mod/core.html#options http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html

Directory Browsing - Apache 2

Source	raised by a passive scanner (Directory Browsing)
CWE ID	548
WASC ID	16
Reference	https://cwe.mitre.org/data/definitions/548.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

Parameter Tampering

Source	raised by an active scanner (Parameter Tampering)
CWE ID	472
WASC ID	20

Secure Pages Include Mixed Content (Including Scripts)

Source	raised by a passive scanner (Secure Pages Include Mixed Content)
CWE ID	311
WASC ID	4
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))

CWE ID 829

Reference

- https://github.com/jquery/jquery/issues/2432
- http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
- http://research.insecurelabs.org/jquery/test/
- https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/
- https://nvd.nist.gov/vuln/detail/CVE-2019-11358
- https://nvd.nist.gov/vuln/detail/CVE-2015-9251
- https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b
- https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

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 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 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

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)

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 Agent Fuzzer

Source	raised by an active scanner (User Agent Fuzzer)
Reference	- https://owasp.org/wstg

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