HRM-Scan-Report

Generated with ZAP on Fri 11 Nov 2022, at 18:35:35

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://fonts.gstatic.com`
- `https://fonts.googleapis.com`
- `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%)	2 (8.3%)	0 (0.0%)	2 (8.3%)
	Medium	0 (0.0%)	2 (8.3%)	6 (25.0%)	1 (4.2%)	9 (37.5%)
	Low	0 (0.0%)	2 (8.3%)	5 (20.8%)	0 (0.0%)	7 (29.2%)
	Informational	0 (0.0%)	1 (4.2%)	3 (12.5%)	2 (8.3%)	6 (25.0%)
	Total	0 (0.0%)	5 (20.8%)	16 (66.7%)	3 (12.5%)	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://fonts.gstatic.com	0 (0)	0 (0)	1 (1)	1 (2)
	https://fonts.googleapis.com	0 (0)	1 (1)	0 (1)	0 (1)
	http://localhost	2 (2)	8 (10)	6 (16)	5 (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
Cross Site Scripting (Reflected)	High	2 (8.3%)
Total		24

Alert type	Risk	Count
SQL Injection - MySQL	High	5 (20.8%)
Absence of Anti-CSRF Tokens	Medium	8 (33.3%)
Application Error Disclosure	Medium	56 (233.3%)
Content Security Policy (CSP) Header Not Set	Medium	71 (295.8%)
Cross-Domain Misconfiguration	Medium	6 (25.0%)
Directory Browsing	Medium	6 (25.0%)
Directory Browsing - Apache 2	Medium	54 (225.0%)
Hidden File Found	Medium	2 (8.3%)
Missing Anti-clickjacking Header	Medium	65 (270.8%)
Vulnerable JS Library	Medium	5 (20.8%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	9 (37.5%)
Cookie No HttpOnly Flag	Low	2 (8.3%)
Total		24

Alert type	Risk	Count
Cookie without SameSite Attribute	Low	2 (8.3%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	16 (66.7%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	138 (575.0%)
Strict-Transport-Security Header Not Set	Low	4 (16.7%)
X-Content-Type-Options Header Missing	Low	124 (516.7%)
GET for POST	Informational	3 (12.5%)
Information Disclosure - Suspicious Comments	Informational	28 (116.7%)
Loosely Scoped Cookie	Informational	2 (8.3%)
Modern Web Application	Informational	7 (29.2%)
Retrieved from Cache	Informational	4 (16.7%)
User Agent Fuzzer	Informational	120 (500.0%)
Total		24

Alerts

Risk=High, Confidence=Medium (2)

http://localhost (2)

Cross Site Scripting (Reflected) (1)

▶ GET http://localhost/hrm/index.php?msg=%3C%2Fh4%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E%3Ch4%3E

SQL Injection - MySQL (1)

▶ POST http://localhost/hrm/controller/login.php

Risk=Medium, Confidence=High (2)

http://localhost (2)

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

▶ GET http://localhost/hrm/

Hidden File Found (1)

▶ GET http://localhost/server-status

Risk=Medium, Confidence=Medium (6)

https://fonts.googleapis.com (1)

Cross-Domain Misconfiguration (1)

▶ GET https://fonts.googleapis.com/css?family=Montserrat:400,700

http://localhost (5)

Application Error Disclosure (1)

▶ GET http://localhost/hrm/controller/

Directory Browsing (1)

▶ GET http://localhost/hrm/controller/

Directory Browsing - Apache 2 (1)

▶ GET http://localhost/hrm/controller/

Missing Anti-clickjacking Header (1)

▶ GET http://localhost/hrm/

Vulnerable JS Library (1)

▶ GET http://localhost/hrm/js/jquery-2.1.4.min.js

Risk=Medium, Confidence=Low (1)

http://localhost (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://localhost/hrm/

Risk=Low, Confidence=High (2)

https://fonts.gstatic.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://fonts.gstatic.com/s/roboto/v30/KFOmCnqEu92Fr1Mu4mxK.woff2

http://localhost (1)

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

▶ GET http://localhost/hrm/css/morris.css

Risk=Low, Confidence=Medium (5)

http://localhost (5)

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

▶ GET http://localhost/hrm

Cookie No HttpOnly Flag (1)

▶ POST http://localhost/hrm/controller/login.php

Cookie without SameSite Attribute (1)

▶ POST http://localhost/hrm/controller/login.php

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

▶ GET http://localhost/hrm/

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

▶ GET http://localhost/hrm/css/morris.css

Risk=Informational, Confidence=High (1)

http://localhost (1)

GET for POST (1)

▶ GET http://localhost/hrm/controller/login.php

Risk=Informational, Confidence=Medium (3)

https://fonts.gstatic.com (1)

Retrieved from Cache (1)

▶ GET https://fonts.gstatic.com/s/roboto/v30/KFOmCnqEu92Fr1Mu4mxK.woff2

http://localhost (2)

Modern Web Application (1)

▶ GET http://localhost/hrm/js/jquery-2.1.4.min.js

User Agent Fuzzer (1)

▶ POST http://localhost/hrm/controller/login.php

Risk=Informational, Confidence=Low (2)

http://localhost (2)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost/hrm/js/jquery-2.1.4.min.js

Loosely Scoped Cookie (1)

▶ POST http://localhost/hrm/controller/login.php

Appendix

Alert types

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

Cross Site Scripting (Reflected)

Source	raised by an active scanner (Cross Site Scripting (Reflected))
CWE ID	79
WASC ID	8
Reference	▪ http://projects.webappsec.org/Cross-Site-Scripting ▪ http://cwe.mitre.org/data/definitions/79.html

SQL Injection - MySQL

Source	raised by an active scanner (SQL Injection)

CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

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/

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

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

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/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://bugs.jquery.com/ticket/11974
- 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 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

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

GET for POST

Source	raised by an active scanner (GET for POST)
CWE ID	16
WASC ID	20

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)

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)

User Agent Fuzzer

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