OnlineBankingDocker-Scan-Report

Generated with ZAP on Tue 15 Nov 2022, at 21:03:10

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://maxcdn.bootstrapcdn.com
- https://fonts.googleapis.com
- http://localhost:8080

(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%)	1 (9.1%)	0 (0.0%)	0 (0.0%)	1 (9.1%)
	Medium	0 (0.0%)	1 (9.1%)	2 (18.2%)	2 (18.2%)	5 (45.5%)
	Low	0 (0.0%)	0 (0.0%)	1 (9.1%)	0 (0.0%)	1 (9.1%)
	Informational	0 (0.0%)	0 (0.0%)	2 (18.2%)	2 (18.2%)	4 (36.4%)
	Total	0 (0.0%)	2 (18.2%)	5 (45.5%)	4 (36.4%)	11 (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.googleapis.com	0 (0)	1 (1)	0 (1)	0 (1)
	http://localhost:8080	1 (1)	4 (5)	1 (6)	4 (10)

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
Vulnerable JS Library	High	1 (9.1%)
Absence of Anti-CSRF Tokens	Medium	4 (36.4%)
Content Security Policy (CSP) Header Not Set	Medium	4 (36.4%)
Total		11

Alert type	Risk	Count
Cross-Domain Misconfiguration	Medium	2 (18.2%)
Hidden File Found	Medium	4 (36.4%)
Vulnerable JS Library	Medium	1 (9.1%)
Cookie without SameSite Attribute	Low	2 (18.2%)
Information Disclosure - Suspicious Comments	Informational	9 (81.8%)
Loosely Scoped Cookie	Informational	3 (27.3%)
Modern Web Application	Informational	3 (27.3%)
User Agent Fuzzer	Informational	96 (872.7%)
Total		11

Alerts

Risk=High, Confidence=High (1)

http://localhost:8080 (1)

Vulnerable JS Library (1)

▶ GET http://localhost:8080/js/bootstrap.min.js

Risk=Medium, Confidence=High (1)

http://localhost:8080 (1)

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

▶ GET http://localhost:8080/index

Risk=Medium, Confidence=Medium (2)

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

Cross-Domain Misconfiguration (1)

▶ GET https://fonts.googleapis.com/css?family=Passion+One

http://localhost:8080 (1)

Vulnerable JS Library (1)

▶ GET http://localhost:8080/js/bootstrap.min.js

Risk=Medium, Confidence=Low (2)

http://localhost:8080 (2)

Absence of Anti-CSRF Tokens (1)

▶ GET http://localhost:8080/index

Hidden File Found (1)

▶ GET http://localhost:8080/.hg

Risk=Low, Confidence=Medium (1)

http://localhost:8080 (1)

Cookie without SameSite Attribute (1)

▶ GET http://localhost:8080/robots.txt

Risk=Informational, Confidence=Medium (2)

http://localhost:8080 (2)

Modern Web Application (1)

▶ GET http://localhost:8080/js/dataTables.bootstrap.min.js

User Agent Fuzzer (1)

▶ POST http://localhost:8080/signup

Risk=Informational, Confidence=Low (2)

http://localhost:8080 (2)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost:8080/js/jquery.easing.min.js

Loosely Scoped Cookie (1)

▶ GET http://localhost:8080/robots.txt

Appendix

Alert types

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

Vulnerable JS Library

Source	raised by a passive scanner (plugin ID: -1)
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

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

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

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

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

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

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)

User Agent Fuzzer

Source raised by an active scanner (User Agent Fuzzer)

Reference

- https://owasp.org/wstg