HBL-Scan-Report

Generated with ZAP on Fri 11 Nov 2022, at 18:10:01

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://push.services.mozilla.com
- http://detectportal.firefox.com
- https://versioncheck-bg.addons.mozilla.org
- https://services.addons.mozilla.org
- https://classify-client.services.mozilla.com
- https://normandy.cdn.mozilla.net
- https://contile.services.mozilla.com
- https://www.hbl.com
- https://download-installer.cdn.mozilla.net
- https://download.mozilla.org
- https://content-signature-2.cdn.mozilla.net
- https://aus5.mozilla.org
- https://shavar.services.mozilla.com
- https://safebrowsing.googleapis.com
- https://firefox.settings.services.mozilla.com

- https://incoming.telemetry.mozilla.org
- http://ocsp.digicert.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%)	1 (4.5%)	1 (4.5%)	2 (9.1%)

	Confidence				
	User Confirmed	High	Medium	Low	Total
Medium	0 (0.0%)	3 (13.6%)	0 (0.0%)	1 (4.5%)	4 (18.2%)
Low	0 (0.0%)	1 (4.5%)	6 (27.3%)	1 (4.5%)	8 (36.4%)
Informational	0 (0.0%)	3 (13.6%)	2 (9.1%)	3 (13.6%)	8 (36.4%)
Total	0 (0.0%)	7 (31.8%)	9 (40.9%)	6 (27.3%)	22 (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://services.addons.mozilla.org	0 (0)	0 (0)	0 (0)	1 (1)
	https://contile.services.mozilla.com	0 (0)	0 (0)	1 (1)	0 (1)

	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://www.hbl.com	2 (2)	4 (6)	7 (13)	6 (19)
https://aus5.mozilla.org	0 (0)	0 (0)	0 (0)	1 (1)

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	High	1 (4.5%)
Cookie Without Secure Flag	High	1 (4.5%)
Absence of Anti-CSRF Tokens	Medium	158 (718.2%)
CSP: Wildcard Directive	Medium	170 (772.7%)
CSP: script-src unsafe-inline	Medium	170
Total		22

Alert type	Risk	Count
		(772.7%)
CSP: style-src unsafe-inline	Medium	170 (772.7%)
CSP: Notices	Low	170 (772.7%)
Cookie No HttpOnly Flag	Low	4 (18.2%)
Cookie Without Secure Flag	Low	679 (3,086.4%)
Cookie with SameSite Attribute None	Low	6 (27.3%)
Cookie without SameSite Attribute	Low	680 (3,090.9%)
Cross-Domain JavaScript Source File Inclusion	Low	149 (677.3%)
Timestamp Disclosure - Unix	Low	22629 (102,859.1%)
X-Content-Type-Options Header Missing	Low	4 (18.2%)
CSP: X-Content-Security-Policy	Informational	170 (772.7%)
CSP: X-WebKit-CSP	Informational	170 (772.7%)
Total		22

Alert type	Risk	Count
Charset Mismatch	Informational	1 (4.5%)
Content Security Policy (CSP) Report-Only Header Found	Informational	153 (695.5%)
Information Disclosure - Sensitive Information in URL	Informational	2 (9.1%)
Information Disclosure - Suspicious Comments	Informational	305 (1,386.4%)
Loosely Scoped Cookie	Informational	3 (13.6%)
Re-examine Cache-control Directives	Informational	14 (63.6%)
Total		22

Alerts

Risk=High, Confidence=Medium (1)

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

Cookie Without Secure Flag (1)

▶ GET https://www.hbl.com

Risk=High, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.hbl.com

Risk=Medium, Confidence=High (3)

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

CSP: Wildcard Directive (1)

▶ GET https://www.hbl.com

CSP: script-src unsafe-inline (1)

▶ GET https://www.hbl.com

CSP: style-src unsafe-inline (1)

▶ GET https://www.hbl.com

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.hbl.com

Risk=Low, Confidence=High (1)

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

CSP: Notices (1)

▶ GET https://www.hbl.com

Risk=Low, Confidence=Medium (6)

https://contile.services.mozilla.com (1)

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

▶ GET https://contile.services.mozilla.com/v1/tiles

https://www.hbl.com (5)

Cookie No HttpOnly Flag (1)

▶ GET https://www.hbl.com

Cookie Without Secure Flag (1)

▶ GET https://www.hbl.com

Cookie with SameSite Attribute None (1)

▶ GET https://www.hbl.com

Cookie without SameSite Attribute (1)

▶ GET https://www.hbl.com

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.hbl.com/about-us

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.hbl.com

Risk=Informational, Confidence=High (3)

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

CSP: X-Content-Security-Policy (1)

▶ GET https://www.hbl.com

CSP: X-WebKit-CSP (1)

▶ GET https://www.hbl.com

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

▶ GET https://www.hbl.com

Risk=Informational, Confidence=Medium (2)

https://services.addons.mozilla.org (1)

Information Disclosure - Sensitive Information in URL (1)

▶ GET https://services.addons.mozilla.org/api/v4/addons/search/?guid=default-theme%40mozilla.org%2Caddons-search-detection%40mozilla.com%2Cgoogle%40search.mozilla.org%2Camazondotcom%40search.mozilla.org%2Cwikipedia%40search.mozilla.org%2Cbing%40search.mozilla.org%2Cddg%40search.mozilla.org%2Cfirefox-compact-light%40mozilla.org%2Cfirefox-compact-

dark%40mozilla.org%2Cfirefox-alpenglow%40mozilla.org%2Cplaymaker-soft-colorway%40mozilla.org%2Cplaymaker-balanced-colorway%40mozilla.org%2Cplaymaker-bold-colorway%40mozilla.org%2Cexpressionist-soft-colorway%40mozilla.org%2Cexpressionist-balanced-colorway%40mozilla.org%2Cexpressionist-bold-colorway%40mozilla.org%2Cvisionary-soft-colorway%40mozilla.org%2Cvisionary-balanced-colorway%40mozilla.org%2Cvisionary-bold-colorway%40mozilla.org%2Cactivist-soft-colorway%40mozilla.org%2Cactivist-balanced-colorway%40mozilla.org%2Cactivist-bold-colorway%40mozilla.org%2Cdreamer-soft-colorway%40mozilla.org%2Cdreamer-balanced-colorway%40mozilla.org%2Cdreamer-bold-colorway%40mozilla.org%2Cinnovator-soft-colorway%40mozilla.org%2Cinnovator-balanced-colorway%40mozilla.org%2Cinnovator-bold-colorway%40mozilla.org%2Cfoxyproxy%40eric.h.jung&lang=en-US

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

Re-examine Cache-control Directives (1)

▶ GET https://www.hbl.com

Risk=Informational, Confidence=Low (3)

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

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.hbl.com

Loosely Scoped Cookie (1)

▶ GET https://www.hbl.com

https://aus5.mozilla.org (1)

Charset Mismatch (1)

▶ GET https://aus5.mozilla.org/update/3/SystemAddons/106.0.3/20221030091646/WINNT_x86_64-msvc-x64/en-US/release/Windows_NT%2010.0.0.0.19044.2130%20(x64)/default/default/update.xml

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 (plugin ID: -1)
CWE ID	352
WASC ID	9
Reference	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery ▪ http://cwe.mitre.org/data/definitions/352.html

Cookie Without Secure Flag

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

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: script-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

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

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+p

olicy

- 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

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

CSP: X-Content-Security-Policy

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: X-WebKit-CSP

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

Charset Mismatch

Source	raised by a passive scanner (Charset Mismatch)

CWE ID	436
WASC ID	15
Reference	▪ http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

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/

Information Disclosure - Sensitive Information in URL

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	200
WASC ID	13

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

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