Amazon.com Scanning Report

Generated with ZAP on Mon 19 Dec 2022, at 15:20:52

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
- https://versioncheck-bg.addons.mozilla.org
- https://services.addons.mozilla.org
- https://aus5.mozilla.org
- https://contile.services.mozilla.com
- https://content-signature-2.cdn.mozilla.net
- https://classify-client.services.mozilla.com
- https://normandy.cdn.mozilla.net
- https://s.amazon-adsystem.com
- https://d2ef20sk9hi1u3.cloudfront.net
- https://dr3fr5q4g2ul9.cloudfront.net
- https://unagi.amazon.com
- https://r6---sn-2uja-pnck.gvt1.com

- `https://redirector.gvt1.com`
- `http://ciscobinary.openh264.org`
- `https://completion.amazon.com`
- `https://fls-na.amazon.com`
- `https://unagi-na.amazon.com`
- `https://assoc-na.associates-amazon.com`
- `https://images-na.ssl-images-amazon.com`
- `https://m.media-amazon.com`
- `https://www.amazon.com`
- `https://tracking-protection.cdn.mozilla.net`
- `https://shavar.services.mozilla.com`
- `https://safebrowsing.googleapis.com`
- `http://ocsp.digicert.com`
- `https://incoming.telemetry.mozilla.org`
- `https://firefox.settings.services.mozilla.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%)	1 (3.1%)	0 (0.0%)	0 (0.0%)	1 (3.1%)
	Medium	0 (0.0%)	4 (12.5%)	3 (9.4%)	1 (3.1%)	8 (25.0%)
	Low	0 (0.0%)	3 (9.4%)	7 (21.9%)	1 (3.1%)	11 (34.4%)
	Informational	0 (0.0%)	1 (3.1%)	4 (12.5%)	7 (21.9%)	12 (37.5%)
	Total	0 (0.0%)	9 (28.1%)	14 (43.8%)	9 (28.1%)	32 (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://aus5.mozilla.org	0 (0)	0 (0)	0 (0)	1 (1)
	https://s.amazon-adsystem.com	0 (0)	1 (1)	0 (1)	0 (1)
	https://r6---sn-2uja-pnck.gvt1.com	0 (0)	0 (0)	0 (0)	1 (1)
	https://assoc-na.associates-amazon.com	0 (0)	0 (0)	1 (1)	0 (1)
	https://m.media-amazon.com	0 (0)	1 (1)	0 (1)	0 (1)
	https://www.amazon.com	1 (1)	4 (5)	6 (11)	8 (19)
	https://shavar.services.mozilla.com	0 (0)	0 (0)	1 (1)	0 (1)
	https://safebrowsing.googleapis.com	0 (0)	0 (0)	1 (1)	0 (1)
	http://ocsp.digicert.com	0 (0)	1 (1)	1 (2)	0 (2)
	https://firefox.settings.services.mozilla.com	0 (0)	1 (1)	1 (2)	2 (4)

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
PII Disclosure	High	2 (6.2%)
Absence of Anti-CSRF Tokens	Medium	1140 (3,562.5%)
CSP: Wildcard Directive	Medium	247 (771.9%)
CSP: script-src unsafe-inline	Medium	247 (771.9%)
CSP: style-src unsafe-inline	Medium	246 (768.8%)
Content Security Policy (CSP) Header Not Set	Medium	111 (346.9%)
Cross-Domain Misconfiguration	Medium	28 (87.5%)
Missing Anti-clickjacking Header	Medium	2 (6.2%)
Vulnerable JS Library	Medium	1 (3.1%)
Application Error Disclosure	Low	1 (3.1%)
Total		32

Alert type	Risk	Count
CSP: Notices	Low	247 (771.9%)
Cookie No HttpOnly Flag	Low	383 (1,196.9%)
Cookie Without Secure Flag	Low	115 (359.4%)
Cookie with SameSite Attribute None	Low	2 (6.2%)
Cookie without SameSite Attribute	Low	387 (1,209.4%)
Cross-Domain JavaScript Source File Inclusion	Low	20 (62.5%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	14 (43.8%)
Strict-Transport-Security Header Not Set	Low	42 (131.2%)
Timestamp Disclosure - Unix	Low	810 (2,531.2%)
X-Content-Type-Options Header Missing	Low	50 (156.2%)
Charset Mismatch	Informational	2 (6.2%)
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	141 (440.6%)
Total		32

Alert type	Risk	Count
Content Security Policy (CSP) Report-Only Header Found	Informational	2 (6.2%)
Content-Type Header Missing	Informational	32 (100.0%)
Information Disclosure - Sensitive Information in URL	Informational	3 (9.4%)
Information Disclosure - Suspicious Comments	Informational	608 (1,900.0%)
Loosely Scoped Cookie	Informational	434 (1,356.2%)
Modern Web Application	Informational	337 (1,053.1%)
Re-examine Cache-control Directives	Informational	248 (775.0%)
Retrieved from Cache	Informational	45 (140.6%)
User Controllable Charset	Informational	1 (3.1%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	102 (318.8%)
Total		32

Alerts

Risk=High, Confidence=High (1)

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

PII Disclosure (1)

▶ GET https://www.amazon.com/s?k=Most+Loved+Gifts

Risk=Medium, Confidence=High (4)

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

CSP: Wildcard Directive (1)

▶ GET https://www.amazon.com/?&tag=googleglobalp-20&ref=pd_sl_7nnedyywlk_e&adgrpid=82342659060&hvpone=&hvptwo=&hvadid=585475370855&hvpos=&hvnetw=g&hvrand=10316527625717988517&hvqmt=e&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9061357&hvtargid=kwd-10573980&hydadcr=2246_13468515&gclid=CjwKCAiAkfucBhBBEiwAFjbkrwgFuXXrcqdNMciAgcSPtqXuDFCWLDvjC_O-sHr5D5q1TvzYLUz71hoCr4EQAvD_BwE

CSP: script-src unsafe-inline (1)

▶ GET https://www.amazon.com/?&tag=googleglobalp-20&ref=pd_sl_7nnedyywlk_e&adgrpid=82342659060&hvpone=&hvptwo=&hvadid=585475370855&hvpos=&hvnetw=g&hvrand=10316527625717988517&hvqmt=e&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9061357&hvtargid=kwd-10573980&hydadcr=2246_13468515&gclid=CjwKCAiAkfucBhBBEiwAFjbkrwgFuXXrcqdNMciAgcSPtqXuDFCWLDvjC_O-sHr5D5q1TvzYLUz71hoCr4EQAvD_BwE

CSP: style-src unsafe-inline (1)

▶ GET https://www.amazon.com/?&tag=googleglobalp-20&ref=pd_sl_7nnedyywlk_e&adgrpid=82342659060&hvpone=&hvptwo=&hvadid=585475370855&hvpos=&hvnetw=g&hvrand=10316527625717988517&hvqmt=e&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9061357&hvtargid=kwd-

10573980&hydadcr=2246_13468515&gclid=CjwKCAiAkfucBhBBEiwAFjbkrwgFuXXrcqdNMciAgcSPtqXuDFCWLDvjC_O-sHr5D5q1TvzYLUz71hoCr4EQAvD_BwE

http://ocsp.digicert.com (1)

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

▶ GET http://ocsp.digicert.com/

Risk=Medium, Confidence=Medium (3)

https://s.amazon-adsystem.com (1)

Missing Anti-clickjacking Header (1)

▶ GET https://s.amazon-adsystem.com/iu3?d=amazon.com&slot=navFooter&a2=0101e3fe592ce18367053b5ff67e3f9aa2aeb50e016f109bc4529c04f40296886d91&old_oo=0&ts=1671379666255&s=AX514rKEGeCVhzxrbH5KtoCmwjqiJ9eHDzXokwC0qQ5S&gdpr_consent=&gdpr_consent_avl=&cb=1671379666255&dcc=t

https://m.media-amazon.com (1)

Vulnerable JS Library (1)

▶ GET https://m.media-amazon.com/images/I/61NeHXhGwSL.js?AUIClients/AmazonUIjQuery&KK9dlo3A

https://firefox.settings.services.mozilla.com (1)

Cross-Domain Misconfiguration (1)

▶ GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?_expected=%221671375434679%22

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.amazon.com/?&tag=googleglobalp-20&ref=pd_sl_7nnedyywlk_e&adgrpid=82342659060&hvpone=&hvptwo=&hvadid=585475370855&hvpos=&hvnetw=g&hvrand=10316527625717988517&hvqmt=e&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9061357&hvtargid=kwd-10573980&hydadcr=2246_13468515&gclid=CjwKCAiAkfucBhBBEiwAFjbkrwgFuXXrcqdNMciAgcSPtqXuDFCWLDvjC_O-sHr5D5q1TvzYLUz71hoCr4EQAvD_BwE

Risk=Low, Confidence=High (3)

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

CSP: Notices (1)

▶ GET https://www.amazon.com/?&tag=googleglobalp-20&ref=pd_sl_7nnedyywlk_e&adgrpid=82342659060&hvpone=&hvptwo=&hvadid=585475370855&hvpos=&hvnetw=g&hvrand=10316527625717988517&hvqmt=e&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9061357&hvtargid=kwd-10573980&hydadcr=2246_13468515&gclid=CjwKCAiAkfucBhBBEiwAFjbkrwgFuXXrcqdNMciAgcSPtqXuDFCWLDvjC_O-sHr5D5q1TvzYLUz71hoCr4EQAvD_BwE

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

Strict-Transport-Security Header Not Set (1)

▶ GET https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch?$ct=application/x-protobuf&key=AIzaSyC7jsptDS3am4tPx4r3nxis7IMjBc5Dovo&$httpMethod=POST&$req=ChUKE25hdmNsaWVudC1hdXRvLWZmb3gaJwgFEAEaGwoNCAUQBhgBIgMwMDEwARDzqQ8aAhgGKQI5YiICIAIoARonCAEQARobCg0IARAGGAEiAzAwMTABEKG_CxoCGAazWaIKIgIgAigBGicIAxABGhsKDQgDEAYYASIDMDAxMAEQ4rQLGgIYBpzhO9giAiACKAEaJwgHEAEaGwoNCAcQBhgBIgMwMDEwARDqmQwaAhgGEk5lvSICIAIoARolCAkQARoZCg0ICRAGGAEiAzAwMTABECAaAhgGSQb-jyICIAIoAQ==

http://ocsp.digicert.com (1)

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

▶ GET http://ocsp.digicert.com/

Risk=Low, Confidence=Medium (7)

https://assoc-na.associates-amazon.com (1)

Cookie with SameSite Attribute None (1)

▶ GET https://assoc-na.associates-amazon.com/abid/um?s=141-2121883-9059715&m=ATVPDKIKX0DER

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

Application Error Disclosure (1)

▶ GET https://www.amazon.com/sitemap.xml

Cookie No HttpOnly Flag (1)

▶ GET https://www.amazon.com/?&tag=googleglobalp-20&ref=pd_sl_7nnedyywlk_e&adgrpid=82342659060&hvpone=&hvptwo=&hvadid=585475370855&hvpos=&hvnetw=g&hvrand=10316527625717988517&hvqmt=e&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9061357&hvtargid=kwd-10573980&hydadcr=2246_13468515&gclid=CjwKCAiAkfucBhBBEiwAFjbkrwgFuXXrcqdNMciAgcSPtqXuDFCWLDvjC_O-sHr5D5q1TvzYLUz71hoCr4EQAvD_BwE

Cookie Without Secure Flag (1)

▶ GET https://www.amazon.com/?&tag=googleglobalp-20&ref=pd_sl_7nnedyywlk_e&adgrpid=82342659060&hvpone=&hvptwo=&hvadid=585475370855&hvpos=&hvnetw=g&hvrand=10316527625717988517&hvqmt=e&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9061357&hvtargid=kwd-10573980&hydadcr=2246_13468515&gclid=CjwKCAiAkfucBhBBEiwAFjbkrwgFuXXrcqdNMciAgcSPtqXuDFCWLDvjC_O-sHr5D5q1TvzYLUz71hoCr4EQAvD_BwE

Cookie without SameSite Attribute (1)

▶ GET https://www.amazon.com/?&tag=googleglobalp-20&ref=pd_sl_7nnedyywlk_e&adgrpid=82342659060&hvpone=&hvptwo=&hvadid=585475370855&hvpos=&hvnetw=g&hvrand=10316527625717988517&hvqmt=e&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9061357&hvtargid=kwd-10573980&hydadcr=2246_13468515&gclid=CjwKCAiAkfucBhBBEiwAFjbkrwgFuXXrcqdNMciAgcSPtqXuDFCWLDvjC_O-sHr5D5q1TvzYLUz71hoCr4EQAvD_BwE

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.amazon.com/gp/goldbox?ref_=nav_cs_gb

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

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

▶ POST https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=107.0&pver=2.2

Risk=Low, Confidence=Low (1)

https://firefox.settings.services.mozilla.com (1)

Timestamp Disclosure - Unix (1)

▶ GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/normandy-recipes-capabilities/changeset?_expected=1671235264186&_since=%221670976064503%22

Risk=Informational, Confidence=High (1)

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

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

▶ GET https://www.amazon.com/portal-migration/hz/glow/get-rendered-toaster?pageType=Gateway&aisTransitionState=in&rancorLocationSource=IP_GEOLOCATION&_=1671379759814

Risk=Informational, Confidence=Medium (4)

https://r6---sn-2uja-pnck.gvt1.com (1)

Information Disclosure - Sensitive Information in URL (1)

▶ GET https://r6---sn-2uja-pnck.gvt1.com/edgedl/widevine-cdm/4.10.2449.0-win-x64.zip?cms_redirect=yes&mh=7o&mip=39.33.241.74&mm=28&mn=sn-2uja-pnck&ms=nvh&mt=1671379471&mv=m&mvi=6&pl=21&rmhost=r5---sn-2uja-pnck.gvt1.com&shardbypass=sd&smhost=r4---sn-2uja-pncr.gvt1.com

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

Content-Type Header Missing (1)

▶ GET https://www.amazon.com/gp/registry/wishlist/*/reserve

Modern Web Application (1)

▶ GET https://www.amazon.com/?&tag=googleglobalp-20&ref=pd_sl_7nnedyywlk_e&adgrpid=82342659060&hvpone=&hvptwo=&hvadid=585475370855&hvpos=&hvnetw=g&hvrand=10316527625717988517&hvqmt=e&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9061357&hvtargid=kwd-10573980&hydadcr=2246_13468515&gclid=CjwKCAiAkfucBhBBEiwAFjbkrwgFuXXrcqdNMciAgcSPtqXuDFCWLDvjC_O-sHr5D5q1TvzYLUz71hoCr4EQAvD_BwE

https://firefox.settings.services.mozilla.com (1)

Retrieved from Cache (1)

▶ GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?_expected=%221671375434679%22

Risk=Informational, Confidence=Low (7)

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

Charset Mismatch (1)

▶ GET https://aus5.mozilla.org/update/6/Firefox/107.0.1/20221128144904/WINNT_x86_64-msvc-x64/en-US/release/Windows_NT%2010.0.0.0.19044.2364%20(x64)/ISET:SSE4_2,MEM:5935/default/default/update.xml

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

Charset Mismatch (Header Versus Meta Content-Type Charset) (1)

▶ GET https://www.amazon.com/Inside-Arab-Mind-Selected-Al-Ansari/dp/B0B3V5K7G7/?_encoding=UTF8&content-id=amzn1.sym.ba25a0fb-eeb9-4762-9c76-8ca869df5234&pd_rd_r=15aae728-3ab4-47d8-a511-7e3c5036c7e2&pd_rd_w=1kpCm&pd_rd_wg=IZv4l&pf_rd_p=ba25a0fb-eeb9-4762-9c76-8ca869df5234&pf_rd_r=2Z9NF44898Q9S5445WS4&ref_=pd_gw_exports_top_sellers_unrec

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.amazon.com/?&tag=googleglobalp-20&ref=pd_sl_7nnedyywlk_e&adgrpid=82342659060&hvpone=&hvptwo=&hvadid=585475370855&hvpos=&hvnetw=g&hvrand=10316527625717988517&hvqmt=e&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9061357&hvtargid=kwd-10573980&hydadcr=2246_13468515&gclid=CjwKCAiAkfucBhBBEiwAFjbkrwgFuXXrcqdNMciAgcSPtqXuDFCWLDvjC_O-sHr5D5q1TvzYLUz71hoCr4EQAvD_BwE

Loosely Scoped Cookie (1)

▶ GET https://www.amazon.com/?&tag=googleglobalp-20&ref=pd_sl_7nnedyywlk_e&adgrpid=82342659060&hvpone=&hvptwo=&hvadid=585475370855&hvpos=&hvnetw=g&hvrand=10316527625717988517&hvqmt=e&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9061357&hvtargid=kwd-10573980&hydadcr=2246_13468515&gclid=CjwKCAiAkfucBhBBEiwAFjbkrwgFuXXrcqdNMciAgcSPtqXuDFCWLDvjC_O-sHr5D5q1TvzYLUz71hoCr4EQAvD_BwE

User Controllable Charset (1)

▶ GET https://www.amazon.com/dp/B07984JN3L?ie=UTF-8&plattr=ACOMFO

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

▶ GET https://www.amazon.com/gp/browse.html?node=16115931011&ref_=nav_cs_registry

https://firefox.settings.services.mozilla.com (1)

Re-examine Cache-control Directives (1)

▶ GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?_expected=%221671375434679%22

Appendix

Alert types

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

PII Disclosure

Source	raised by a passive scanner (PII Disclosure)
CWE ID	359
WASC ID	13

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

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

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://nvd.nist.gov/vuln/detail/CVE-2012-6708 ▪ https://github.com/jquery/jquery/issues/2432 ▪ http://research.insecurelabs.org/jquery/test/

- http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
- http://bugs.jquery.com/ticket/11290
- 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/

Application Error Disclosure

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

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+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

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

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

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

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

Charset Mismatch (Header Versus Meta Content-Type Charset)

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/

Content-Type Header Missing

Source	raised by a passive scanner (Content-Type Header Missing)
CWE ID	345
WASC ID	12
Reference	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx

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

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/

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 Controllable Charset

Source	raised by a passive scanner (User Controllable Charset)
CWE ID	20
WASC ID	20

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