Scan Summary

Host:	open.spotify.com
Scan ID #:	30880603
Start Time:	November 13, 2022 7:12 PM
Duration:	4 seconds
Score:	65/100
Tests Passed:	8/11

Recommendation

Initiate Rescan

You’re doing a wonderful job so far!

Did you know that a strong Content Security Policy (CSP) policy can help protect your website against malicious cross-site scripting attacks?

- Mozilla Web Security Guidelines (Content Security Policy)
- An Introduction to Content Security Policy
- Google CSP Evaluator
- Mozilla Laboratory CSP Generator

Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

Test Scores

Test	Pass	Score	Reason
Content Security Policy	✗	-20	Content Security Policy (CSP) implemented unsafely. This includes `'unsafe-inline'` or `data:` inside `script-src`, overly broad sources such as https: inside `object-src` or `script-src`, or not restricting the sources for `object-src` or `script-src`.
Cookies	✓	+5	All cookies use the `Secure` flag, session cookies use the `HttpOnly` flag, and cross-origin restrictions are in place via the `SameSite` flag
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)

Test	Pass	Score	Reason
HTTP Strict Transport Security	✓	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)
Redirection	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)
Subresource Integrity	✗	-5	Subresource Integrity (SRI) not implemented, but all external scripts are loaded over HTTPS
X-Content-Type-Options	✓	0	X-Content-Type-Options header set to `"nosniff"`
X-Frame-Options	✓	+5	X-Frame-Options (XFO) implemented via the CSP `frame-ancestors` directive
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented

Content Security Policy Analysis

Test	Pass
Blocks execution of inline JavaScript by not allowing `'unsafe-inline'` inside `script-src`	✗
Blocks execution of JavaScript's `eval()` function by not allowing `'unsafe-eval'` inside `script-src`	✗
Blocks execution of plug-ins, using `object-src` restrictions	✗
Blocks inline styles by not allowing `'unsafe-inline'` inside `style-src`	✗
Blocks loading of active content over HTTP or FTP	✓
Blocks loading of passive content over HTTP or FTP	✓
Clickjacking protection, using `frame-ancestors`	✓
Deny by default, using `default-src 'none'`	✗
Restricts use of the `<base>` tag by using `base-uri 'none'`, `base-uri 'self'`, or specific origins	✗
Restricts where `<form>` contents may be submitted by using `form-action 'none'`, `form-action 'self'`, or specific URIs	✗
Uses CSP3's `'strict-dynamic'` directive to allow dynamic script loading (optional)	–

Looking for additional help? Check out Google's CSP Evaluator!

Cookies

Name	Expires	Path	Secure ⓘ	HttpOnly ⓘ	SameSite ⓘ	Prefixed ⓘ
sp_landing	November 12, 1671 9:00 AM	/	✓	✓	None	✗

Name	Expires	Path	Secure ()	HttpOnly ()	SameSite ()	Prefixed ()

Grade History

Date	Score	Grade
July 16, 2021 7:52 PM	65	B-
June 24, 2021 5:42 AM	45	C-
April 28, 2021 5:02 AM	65	B-
July 10, 2020 2:02 PM	45	C-
February 3, 2019 4:21 PM	65	B-
January 15, 2019 12:07 PM	40	D+
November 9, 2018 4:58 AM	65	B-
October 26, 2017 10:02 PM	40	D+
May 21, 2016 1:16 PM	35	D

Raw Server Headers

Header	Value
Alt-Svc:	h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Transfer-Encoding:	chunked
Via:	HTTP/2 edgeproxy, 1.1 google
content-encoding:	gzip
content-security-policy:	script-src 'self' 'unsafe-eval' blob: open.spotifycdn.com open-review.spotifycdn.com quicksilver.scdn.co www.google-analytics.com www.googletagmanager.com static.ads-twitter.com analytics.twitter.com s.pinimg.com sc-static.net https://www.google.com/recaptcha/ cdn.ravenjs.com connect.facebook.net www.gstatic.com sb.scorecardresearch.com pixel-static.spotify.com optimize.google.com cdn.cookielaw.org geolocation.onetrust.com www.googleoptimize.com www.fastly-insights.com static.hotjar.com script.hotjar.com https://www.googleadservices.com/pagead/conversion_async.js https://www.googleadservices.com/pagead/conversion/ https://analytics.tiktok.com/i18n/pixel/sdk.js https://analytics.tiktok.com/i18n/pixel/identify.js https://analytics.tiktok.com/i18n/pixel/config.js https://www.redditstatic.com/ads/pixel.js cdn.speedcurve.com 'sha256-WfsTi7oVogdF9vq5d14s2birjvCglqWF842fyHhzoNw=' 'sha256-KRzjHxCdT8icNaDOqPBdY0AlKiIh5F8r4bnbe1PQwss=' 'sha256-Z5wh7XXSBR1+mTxLSPFhywCZJt77+uP1GikAgPIsu2s='; frame-ancestors 'self';
content-type:	text/html; charset=utf-8
date:	Mon, 14 Nov 2022 00:12:13 GMT
server:	envoy

Header	Value
set-cookie:	sp_t=7b2f975b561b3b2b8ddb248559664d63; path=/; expires=Tue, 14 Nov 2023 00:12:13 GMT; domain=.spotify.com; samesite=none; secure, sp_landing=https%3A%2F%2Fopen.spotify.com%2F%3Fsp_cid%3D7b2f975b561b3b2b8ddb248559664d63%26device%3Ddesktop; path=/; expires=Tue, 15 Nov 2022 00:12:13 GMT; domain=.spotify.com; samesite=none; secure; httponly
sp-trace-id:	c62bce8d9aef3712
strict-transport-security:	max-age=31536000
vary:	Accept-Encoding,Accept-Encoding
x-content-type-options:	nosniff
x-envoy-upstream-service-time:	41