


Scan Summary



Host:

josebrouwer.me

Scan ID #:

45017045 (unlisted)

Start Time:

November 29, 2023 9:00 PM

Duration:

41 seconds

Score:

110/100

Tests Passed:

11/11

Recommendation

Initiate Rescan

You're on the home stretch!

The use of Referrer Policy can help protect the privacy of your users by restricting the information that browsers provide when accessing resources kept on other sites.

- [Mozilla Web Security Guidelines \(Referrer Policy\)](#)

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

Test Scores					
Test	Pass	Score	Reason	Info	
Content Security Policy	✓	+5	Content Security Policy (CSP) implemented without 'unsafe-inline' or 'unsafe-eval'	ⓘ	
Cookies	—	0	No cookies detected	ⓘ	
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)	ⓘ	
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) is implemented and all scripts are loaded securely	ⓘ	
X-Content-Type-Options	✓	0	X-Content-Type-Options header set to "nosniff"	ⓘ	
X-Frame-Options	✓	0	X-Frame-Options (XFO) header set to SAMEORIGIN or DENY	ⓘ	
X-XSS-Protection	✓	0	X-XSS-Protection header set to "1; mode=block"	ⓘ	

Content Security Policy Analysis

Test	Pass	Info
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!

Grade History		
Date	Score	Grade
November 28, 2023 2:36 PM	110	A+
November 21, 2023 9:06 PM	80	B+
November 21, 2023 8:58 PM	60	C+
November 17, 2023 8:18 PM	80	B+
November 17, 2023 7:24 PM	60	C+
October 13, 2023 4:08 PM	80	B+
October 13, 2023 3:38 PM	60	C+
October 13, 2023 2:55 PM	0	F
September 21, 2023 3:14 PM	20	F

Raw Server Headers

Header	Value
Connection:	keep-alive
Content-Encoding:	gzip
Content-Security-Policy:	default-src 'self' https://cdn.jsdelivr.net https://lh3.googleusercontent.com https://hacker-news.firebaseio.com; script-src 'self' https://cdn.jsdelivr.net;
Content-Type:	text/html; charset=utf-8
Date:	Thu, 30 Nov 2023 02:01:08 GMT
Server:	nginx/1.18.0 (Ubuntu)
Strict-Transport-Security:	max-age=31536000
Transfer-Encoding:	chunked
Vary:	Cookie
X-Content-Type-Options:	nosniff
X-Frame-Options:	DENY
X-XSS-Protection:	1; mode=block