


Scan Summary



Host:	www.irobot.com
Scan ID #:	52700605
Start Time:	June 25, 2024 3:07 PM
Duration:	5 seconds
Score:	20/100
Tests Passed:	8/11

Recommendation

Initiate Rescan

Fantastic work using HTTPS! Did you know that you can ensure users never visit your site over HTTP accidentally?

HTTP Strict Transport Security tells web browsers to only access your site over HTTPS in the future, even if the user attempts to visit over HTTP or clicks an `http://` link.

- [Mozilla Web Security Guidelines \(HSTS\)](#)
- [MDN on HTTP Strict Transport Security](#)

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 Strict Transport Security	✗	-10	HTTP Strict Transport Security (HSTS) header set to less than 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)

Test	Pass	Score	Reason
Subresource Integrity	✗	-50	Subresource Integrity (SRI) not implemented, and external scripts are loaded over HTTP or use protocol-relative URLs via <code>src="//..."</code>
X-Content-Type-Options	✓	0	X-Content-Type-Options header set to <code>"nosniff"</code>
X-Frame-Options	✓	+5	X-Frame-Options (XFO) implemented via the CSP <code>frame-ancestors</code> directive
X-XSS-Protection	✓	0	Deprecated X-XSS-Protection header not implemented

Content Security Policy Analysis

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

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

Cookies

Name	Expires	Path	Secure.0	HttpOnly.0	SameSite.0	Prefixed.0
__cq_dnt	Session	/	✓	✗	None	✗
cqcid	Session	/	✓	✗	None	✗
cquid	Session	/	✓	✗	None	✗
dw_dnt	Session	/	✓	✗	None	✗
dwac_ddcb22018c454a1247eeba52a2	Session	/	✓	✗	None	✗

Name	Expires	Path	Secure.0	HttpOnly.0	SameSite.0	Prefixed.0
dwanonymous_oe12ec9a6a9932971a094fc91c1fbbba	July 21, 1741 6:00 PM	/	✓	✗	None	✗
dwsid	Session	/	✓	✓	None	✗
sid	Session	/	✓	✗	None	✗

Grade History		
Date	Score	Grade
June 4, 2024 7:21 PM	20	F
April 16, 2019 4:34 AM	0	F

Raw Server Headers	
Header	Value
CF-Cache-Status:	DYNAMIC
CF-RAY:	899795eafb12eb6f-SEA
Cache-Control:	no-cache, no-store, must-revalidate
Connection:	keep-alive
Content-Encoding:	gzip
Content-Security-Policy:	frame-ancestors 'self'
Content-Type:	text/html; charset=UTF-8
Date:	Tue, 25 Jun 2024 20:07:46 GMT
Expires:	Thu, 01 Dec 1994 16:00:00 GMT
Pragma:	no-cache
Server:	cloudflare
Set-Cookie:	dwac_ddcb22018c454a1247eeba52a2=uWn_7rHC2gjyaTOB7PFCEt2-Ndbe17qolNI%3D dw-only USD false US%2FEastern true; Path=/; Secure; SameSite=None, cqcid=dehafBbhtJNoskWwfdhoySKVcy; Path=/; Secure; SameSite=None, cquid= ; Path=/; Secure; SameSite=None, sid=uWn_7rHC2gjyaTOB7PFCEt2-Ndbe17qolNI; Path=/; Secure; SameSite=None, dwanonymous_oe12ec9a6a9932971a094fc91c1fbbba=dehafBbhtJNoskWwfdhoySKVcy; Version=1; Comment="Demandware anonymous cookie for site Sites-iRobotUS-Site"; Max-Age=15552000; Expires=Sun, 22 Dec 2024 20:07:45 GMT; Path=/; Secure; SameSite=None, __cq_dnt=0; Path=/; Secure; SameSite=None, dw_dnt=0; Path=/; Secure; SameSite=None, dwsid=cKBrd_knvNKB EqRnDzm8kxR3oU-WMtxu_amJAeRd2ZTANKYVnMPwyWNYnrmUA7xizAxyTx7MN5RZD96scgyC3g==; path=/; HttpOnly; Secure; SameSite=None
Strict-Transport-Security:	max-age=300

Header	Value
Transfer-Encoding:	chunked
X-Content-Type-Options:	nosniff
vary:	accept-encoding
x-dw-request-base-id:	alBgWB32emYBAAB_