


# Scan Summary



Host:	www.apple.com
Scan ID #:	38925309
Start Time:	June 24, 2023 2:24 AM
Duration:	3 seconds
Score:	75/100
Tests Passed:	9/11

# Recommendation

Initiate Rescan

You're doing a great job with HTTPS and HTTP Strict Transport Security!

Since you're now only allowing connections over HTTPS, consider using the **Secure** flag to protect your cookies against their accidental transmission over HTTP. Furthermore, the use of **HttpOnly** protects your session cookies from malicious JavaScript.

- [Mozilla Web Security Guidelines \(cookies\)](#)

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

# Test Scores

Test	Pass	Score	Reason
<a href="#">Content Security Policy</a>	✗	-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.
<a href="#">Cookies</a>	✗	-5	Cookies set without using the Secure flag, but transmission over HTTP prevented by HSTS
<a href="#">Cross-origin Resource Sharing</a>	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers
<a href="#">HTTP Public Key Pinning</a>	—	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)
<a href="#">HTTP Strict Transport Security</a>	✓	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)
<a href="#">Redirection</a>	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS

Test	Pass	Score	Reason
<a href="#">Referrer Policy</a>	—	0	Referrer-Policy header set to "no-referrer-when-downgrade"
<a href="#">Subresource Integrity</a>	—	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin
<a href="#">X-Content-Type-Options</a>	✓	0	X-Content-Type-Options header set to "nosniff"
<a href="#">X-Frame-Options</a>	✓	0	X-Frame-Options (XFO) header set to SAMEORIGIN or DENY
<a href="#">X-XSS-Protection</a>	✓	0	X-XSS-Protection header set to "1; mode=block"

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.Q	HttpOnly.Q	SameSite.Q	Prefixed.Q
geo	Session	/	✗	✗	✗	✗

Grade History

Click to View

Raw Server Headers

Header	Value
Cache-Control:	max-age=0
Connection:	keep-alive
Content-Encoding:	gzip
Content-Length:	36308
Content-Security-Policy:	default-src 'self' blob: data: *.akamaized.net *.apple.com *.apple-mapkit.com *.cdn-apple.com *.organicfruitapps.com; child-src blob: embed.music.apple.com embed.podcasts.apple.com https://recyclingprogram.apple.com swdlp.apple.com www.apple.com www.instagram.com platform.twitter.com www.youtube-nocookie.com; img-src 'unsafe-inline' blob: data: *.apple.com *.apple-mapkit.com *.cdn-apple.com *.mzstatic.com; script-src 'unsafe-inline' 'unsafe-eval' blob: *.apple.com *.apple-mapkit.com www.instagram.com platform.twitter.com; style-src 'unsafe-inline' *.apple.com
Content-Type:	text/html; charset=utf-8
Date:	Fri, 23 Jun 2023 23:24:33 GMT
Expires:	Fri, 23 Jun 2023 23:24:33 GMT
Referrer-Policy:	no-referrer-when-downgrade
Server:	Apple
Set-Cookie:	geo=US; path=/; domain=.apple.com
Strict-Transport-Security:	max-age=31536000; includeSubdomains; preload
Vary:	Accept-Encoding
X-Cache:	TCP_HIT from a23-67-79-231.deploy.akamaitechnologies.com (AkamaiGHost/11.1.2-48827901) (-)
X-Content-Type-Options:	nosniff
X-Frame-Options:	SAMEORIGIN
X-Xss-Protection:	1; mode=block