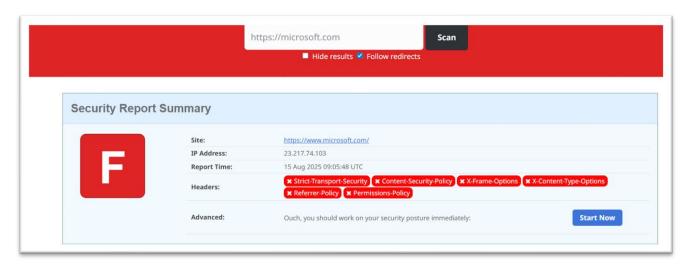
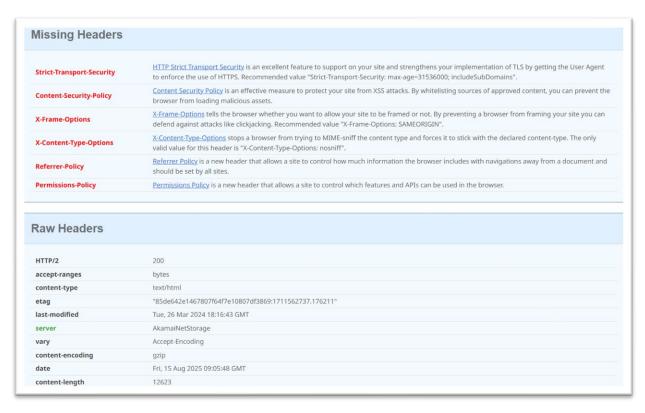
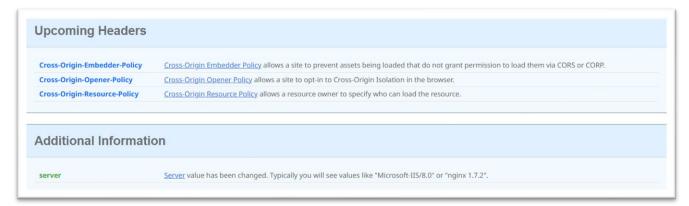
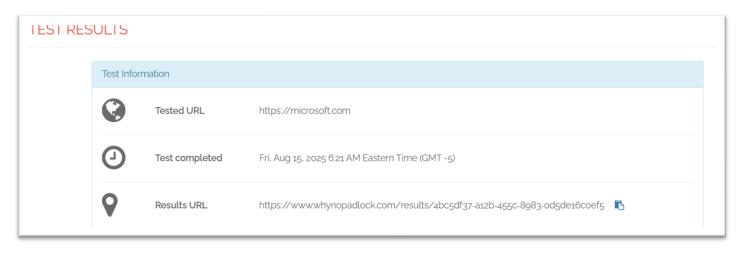
https://microsoft.com using securityheaders.com

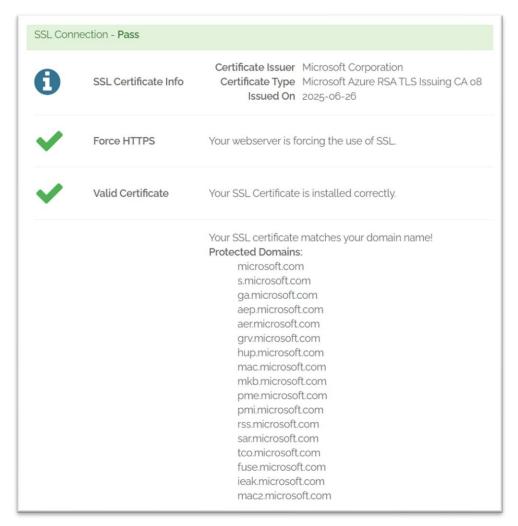


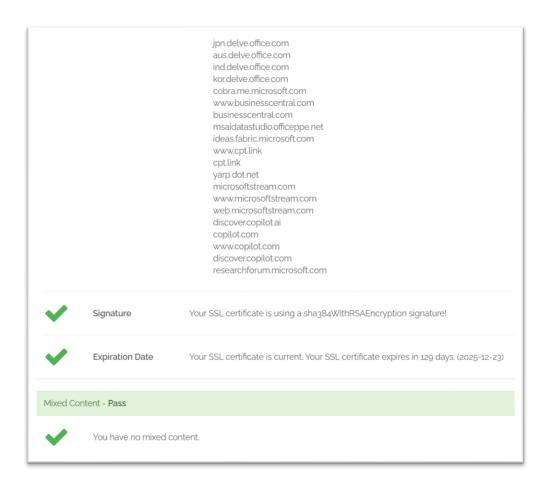




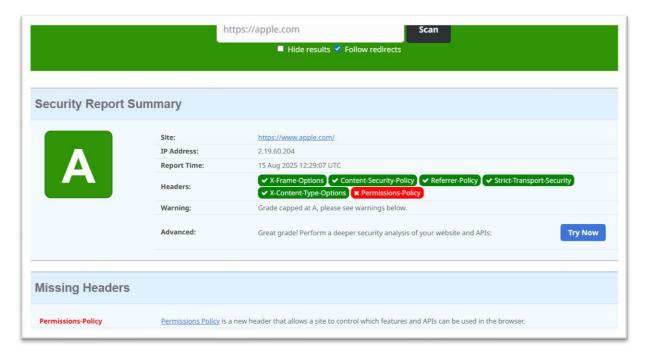
https://microsoft.com using whynopadlock.com







https://apple.com using securityheaders.com





Raw Headers	
HTTP/2	200
server	Apple
content-type	text/html; charset=utf-8
set-cookie	ac_ss=a2926c:1:1770812947; expires=Wed, 11-Feb-2026 12:29:07 GMT; path=/; secure; HttpOnly
set-cookie	geo=IE; path=/; domain=.apple.com
x-frame-options	SAMEORIGIN
vary	X-MVT-Story-Data, Accept-Encoding
x-mvt-analytics-data	[{"experimentId":"a2926c","variationId":"B"}]
x-mvt-story-data	us-7-2025-homepage-ipad-family-content:B
content-security-policy	default-src 'self' blob: data: *.akamaized.net *.apple.com *.apple-mapkit.com *.cdn-apple.com *.organicfruitapps.com; child-src blob: mailto embed.music.apple.com embed.podcasts.apple.com https://smb.apple.com https://smb.apple.com https://smb.apple.com swdlp.apple.com www.apple.com www.instagram.com platform.twitteccom www.youtube-nocookie.com; img-src 'unsafe-inline' blob: data: *.apple.com *.apple.applit.com *.dn-apple.com *.apple.applit.com *
referrer-policy	no-referrer-when-downgrade
strict-transport-security	max-age=31536000; includeSubdomains; preload
x-content-type-options	nosniff
x-xss-protection	1; mode=block
content-encoding	gzip
cache-control	max-age=290
expires	Fri, 15 Aug 2025 12:33:57 GMT
date	Fri, 15 Aug 2025 12:29:07 GMT

Jpcoming Headers	
Cross-Origin-Embedder-Policy	Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	<u>Cross-Origin Resource Policy</u> allows a resource owner to specify who can load the resource.
dditional Informati	Server value has been changed. Typically you will see values like "Microsoft-IIS/8.0" or "nginx 1.7.2".
r-frame-options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you car defend against attacks like clickjacking.
content-security-policy	Content Security Policy is an effective measure to protect your site from X55 attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets. Analyse this policy in more detail. You can sign up for a free account on Report URI to collect reports about problems on your site.
referrer-policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
eterrer-policy	
	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS.
strict-transport-security x-content-type-options	

https://apple.com using whynopadlock.com

