Scan your site now

https://safetynetbeta.com Scan

Hide results Follow redirects

Security Report Summary

A

Site:	https://safetynetbeta.com/
IP Address:	172.67.178.8
Report Time:	03 Jan 2026 05:10:55 UTC
Headers:	✔ Content-Security-Policy ✔ Permissions-Policy ✔ Referrer-Policy ✔ Strict-Transport-Security ✔ X-Content-Type-Options ✔ X-Frame-Options
Warning:	Grade capped at A, please see warnings below.
Advanced:	Great grade! Perform a deeper security analysis of your website and APIs: Try N

Warnings

Content-Security-Policy	This policy contains 'unsafe-inline' which is dangerous in the script-src directive. This policy contains 'unsafe-eval' which is dangerous ir directive.

Raw Headers

HTTP/2	200
date	Sat, 03 Jan 2026 05:10:55 GMT
content-type	text/html; charset=utf-8
nel	{"**report_to**":"cf-nel","**success_fraction**":0.0,"**max_age**":604800}
access-control-allow-origin	*
age	0
cache-control	public, max-age=0, must-revalidate
content-disposition	inline
report-to	{"**group**":"cf-nel","**max_age**":604800,"**endpoints**":[{"**url**":"https://a.nel.cloudflare.com/report/v4?s=4gFt4VaUCPnyapOP%2B%2FvW28Dgma7KF%2FxH0W5g%2BPjFdBm7YUe6XBfP51b1bj6ePNmG0easPU1Q381lBOvHbFgCANDgxm8oNPjfP%2B"}]}
content-security-policy	**default-src** 'self'; **script-src** 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.tailwindcss.com https://www.google.com https://www.gstatic.c https://challenges.cloudflare.com https://static.cloudflareinsights.com https://vercel.live; **style-src** 'self' 'unsafe-inline' https://fonts.goo **font-src** 'self' https://fonts.gstatic.com; **img-src** 'self' data: https:; **connect-src** 'self' https://*.supabase.co https://www.google.com https://www.gstatic.com https://challenges.cloudflare.com https://static.cloudflareinsights.com https://safetynet-signup.campbell-mccord.workers.dev https://vercel.live; **frame-src** https://www.google.com https://www.gstatic.com https://challenges.cloudflare.com https://vercel.live; **frame-ancestors** 'none';
vary	accept-encoding
last-modified	Sat, 03 Jan 2026 05:10:55 GMT
permissions-policy	**camera**=(), **microphone**=(), **geolocation**=()
referrer-policy	**strict-origin-when-cross-origin**
server	cloudflare
strict-transport-security	**max-age**=31536000; **includeSubDomains**
x-content-type-options	**nosniff**

x-frame-options	**DENY**
x-vercel-cache	HIT
x-vercel-id	dub1::87br5-1767417055240-2f23876dc7b1
x-xss-protection	**1**; **mode**=block
cf-cache-status	DYNAMIC
content-encoding	gzip
cf-ray	9b7ffe131ee14ff2-DUB
alt-svc	h3=":443"; ma=86400

Upcoming 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 CORF
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	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

Additional Information

nel	Network Error Logging is a new header that instructs the browser to send reports during various network or application errors. You ca free account on Report URI to collect these reports.
access-control-allow-origin	This is a very lax CORS policy. Such a policy should only be used on a public CDN.
report-to	Report-To enables the Reporting API. This allows a website to collect reports from the browser about various errors that may occur. You for a free account on Report URI to collect these reports.
content-security-policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you c browser from loading malicious assets. Analyse this policy in more detail. You can sign up for a free account on Report URI to collect re problems on your site.
permissions-policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.
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 c should be set by all sites.
server	Server value has been changed. Typically you will see values like "Microsoft-IIS/8.0" or "nginx 1.7.2".
strict-transport-security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting th to enforce the use of HTTPS.
x-content-type-options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type valid value for this header is "X-Content-Type-Options: nosniff".
x-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 you defend against attacks like clickjacking.
x-xss-protection	X-XSS-Protection sets the configuration for the XSS Auditor built into older browsers. The recommended value was "X-XSS-Protection: 1 but you should now look at Content Security Policy instead.