Security Headers

by snyk

Scan your site now

https://cdbougainvillea.netlify. **Scan**

☐ Hide results ☑ Follow redirects

Security Report Summary

A

Site:	https://cdbougainvillea.netlify.app/
IP Address:	35.157.26.135
Report Time:	24 Jul 2025 12:07:50 UTC
Headers:	✓ Permissions-Policy ✓ Referrer-Policy ✓ Strict-Transport-Security ✓ X-Content-Type-Options ✓ X-Frame-Options ✗ Content-Security-Policy
Advanced:	Great grade! Perform a deeper security analysis of your website and APIs: **Try Now**

Missing Headers

Content-Security-Policy Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.

Raw Headers

HTTP/2	200
accept-ranges	bytes
age	0
cache-control	public,max-age=0,must-revalidate
cache-status	"Netlify Edge"; fwd=miss
content-encoding	gzip
content-type	text/html; charset=UTF-8
cross-origin-resource-policy	**same-origin**
date	Thu, 24 Jul 2025 12:07:49 GMT
etag	"b6b7b240e99151021ba414fae7a7e677-ssl-df"
permissions-policy	**camera**=(), **microphone**=(), **geolocation**=()
referrer-policy	**strict-origin-when-cross-origin**
server	Netlify
strict-transport-security	**max-age**=31536000; **includeSubDomains**; **preload**
vary	Accept-Encoding
x-content-type-options	**nosniff**
x-frame-options	**DENY**
x-nf-request-id	01K0Y5A96PJGTEFJ1TQ61PAPNR
content-length	460

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 CORP.

Cross-Origin-Opener-Policy Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.

Additional Information

cross-origin-resource-policy Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

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 document and 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 the User Agent 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. The only 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 your site you can defend against attacks like clickjacking.