Scan your site now

https://cybersecurite50.wordpress.com/ Scan

Hide results Follow redirects

Security Report Summary

D

Site:	https://cybersecurite50.wordpress.com/
IP Address:	192.0.78.13
Report Time:	27 Jul 2025 22:47:08 UTC
Headers:	✔ Strict-Transport-Security ✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Optic ✖ Referrer-Policy ✖ Permissions-Policy
Advanced:	Your site could be at risk, let's perform a deeper security analysis of your site and APIs: Start

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 c browser from loading malicious assets.
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. Recommended value "X-Frame-Options: SAMEORIGIN".
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-typ valid value for this header is "X-Content-Type-Options: nosniff".
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.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Raw Headers

HTTP/2	200
server	nginx
date	Sun, 27 Jul 2025 22:47:08 GMT
content-type	text/html; charset=UTF-8
vary	Accept-Encoding
x-hacker	Want root? Visit join.a8c.com/hacker and mention this header.
host-header	WordPress.com
vary	accept, content-type, cookie
link	<https://wp.me/gGues>; rel=shortlink
content-encoding	gzip
x-ac	2.lhr _dfw MISS
server-timing	a8c-cdn, dc;desc=lhr, cache;desc=MISS;dur=324.0
alt-svc	h3=":443"; ma=86400
strict-transport-security	**max-age**=31536000

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

server	This Server header seems to advertise the software being run on the server but you can remove or change this value.
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.