Security Headers

Powered by

Home Abc

Scan your site now

ourshopee.com Scan

Hide results Follow redirects

Security Report Summary

F

Site:	https://www.ourshopee.com/
IP Address:	2606:4700:3108::ac42:28c5
Report Time:	07 Jul 2024 09:51:43 UTC
Headers:	☐ Strict-Transport-Security ☐ Content-Security-Policy ☐ X-Frame-Options ☐ X-Content-Type-Options ☐ Referrer-Policy ☐ Permissions-Policy
Advanced:	Ouch, you should work on your security posture immediately: Start Now

Missing Headers

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 t the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
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 th er 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 your site you can d 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-type. The only vali 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 document and 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
date	Sun, 07 Jul 2024 09:51:43 GMT
content-type	text/html
last-modified	Tue, 07 May 2024 13:53:36 GMT
cache-control	max-age=2678400
expires	Wed, 07 Aug 2024 09:51:42 GMT
cf-cache-status	DYNAMIC
report-to	{"**endpoints**":[{"**url**":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=kxTd%2FABUTHOsoGhJ5%2BgLTkj5W6ISNaB7jFH2TdGfDt6gMJz7Ek1%2BmG7Ptul2PZwz26rYozNzwUtxZit6YpPxU7C6%2B8P4RYL%2FFXknJda%2BVuvl08PjWPJYsS%2FZqqy4m25JKBE3dOxeOfKzoTx6kURf"}],"**group**":"cf-nel","**max_age**":604800}
nel	{"**success_fraction**":0,"**report_to**":"cf-nel","**max_age**":604800}
server	cloudflare
cf-ray	89f6f001fcdd7e2a-SJC

content-encoding	gzip
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 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	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

Additional Information

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 can sign up account on Report URI to collect these reports.
nel	Network Error Logging is a new header that instructs the browser to send reports during various network or application errors. You can sign up for a f count on Report URI to collect these reports.
server	Server value has been changed. Typically you will see values like "Microsoft-IIS/8.0" or "nginx 1.7.2".