Security Headers

by Probely, a snyk Business

- About
- API
- Scan your site now

Hide results Follow redirects

Security Report Summary

D

Site:	https://hariyoilam.shop/
IP Address:	92.112.189.218
Report Time:	01 Dec 2024 23:17:47 UTC
Headers:	• Content-Security-Policy • Strict-Transport-Security • X-Frame-Options • X-Content-Type-Options • Referrer-Policy • Permissions-Policy

Advanced:	Your site could be at risk, let's perform a deeper security analysis of your site and APIs:

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 to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
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. 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 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 document and 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
x-powered-by	PHP/8.2.22
content-type	text/html; charset=UTF-8
link	<https://hariyoilam.shop/wp-json/>; rel="https://api.w.org/"
link	<https://hariyoilam.shop/wp-json/wp/v2/pages/95>; rel="alternate"; title="JSON"; type="application/json"
link	<https://hariyoilam.shop/>; rel=shortlink
etag	"523-1732892906;gz"

x-litespeed-cache	hit
content-encoding	gzip
vary	Accept-Encoding
date	Sun, 01 Dec 2024 23:17:46 GMT
server	LiteSpeed
platform	hostinger
panel	hpanel
content-security-policy	upgrade-insecure-requests
alt-svc	h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

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

x-powered-by	X-Powered-By can usually be seen with values like "PHP/5.5.9-1ubuntu4.5" or "ASP.NET". Trying to minimise the amount of information you give out about your server is a good idea. This header should be removed or the value changed.
server	Server value has been changed. Typically you will see values like "Microsoft-IIS/8.0" or "nginx 1.7.2".

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. 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.

-
-
-