Security Headers

Powered by

Home Abc

Scan your site now

vendasta.com Scan

Hide results Follow redirects

Security Report Summary

E

Site:	http://www.vendasta.com/ - (Scan again over https)
IP Address:	151.101.41.91
Report Time:	07 Jul 2024 09:50:53 UTC
Headers:	☐ X-Content-Type-Options ☐ Content-Security-Policy ☐ X-Frame-Options ☐ Referrer-Policy ☐ Permissions
Warning:	Grade capped at A, please see warnings below.
Advanced:	Your site could be at risk, let's perform a deeper security analysis of your site and APIs: Start 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 tl 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".
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.

Warnings

Site is using HTTP	This site was served over HTTP and did not redirect to HTTPS.

Raw Headers

HTTP/1.1	200 OK
Connection	keep-alive
Content-Length	79576
Content-Type	text/html; charset=UTF-8
Cache-Control	max-age=60
Link	<https://www.vendasta.com/wp-json/>; rel="https://api.w.org/"
Link	<https://www.vendasta.com/wp-json/wp/v2/pages/80964>; rel="alternate"; type="application/json"
Link	<https://www.vendasta.com/>; rel=shortlink
X-Tec-Api-Origin	https://www.vendasta.com
X-Tec-Api-Root	https://www.vendasta.com/wp-json/tribe/events/v1/

X-Tec-Api-Version	v1
Server	website-pro/8.8.0
x-content-type-options	**nosniff**
x-srcache-fetch-status	HIT
x-xss-protection	**1**; **mode**=block
Content-Encoding	gzip
Via	1.1 google, 1.1 varnish
Accept-Ranges	bytes
Age	353
Date	Sun, 07 Jul 2024 09:50:53 GMT
X-Served-By	cache-sjc10082-SJC
X-Cache	HIT
X-Cache-Hits	0
X-Timer	S1720345853.278786,VS0,VE1
Vary	Accept-Encoding
alt-svc	h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":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

Server	Server value has been changed. Typically you will see values like "Microsoft-IIS/8.0" or "nginx 1.7.2".
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".
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; mode=blo you should now look at Content Security Policy instead.