Security Headers

Home Abc

Sponsored by

Scan your site now

https://certvet-front.us-east-1.elasticbeai Scan

Hide results Follow redirects

Security Report Summary

A

Site:	https://certvet-front.us-east-1.elasticbeanstalk.com/
IP Address:	34.197.163.255
Report Time:	29 Nov 2022 02:11:59 UTC
Headers:	✔ X-Frame-Options ✔ X-Content-Type-Options ✔ Referrer-Policy ✔ Permissions-Policy ✔ Strict-Transport-Security ✖ Content-Security-Policy

Supported By

Probely	Great grade! Perform a deeper security analysis of your website and APIs:	Try Now

Raw Headers

HTTP/2	200
date	Tue, 29 Nov 2022 02:11:59 GMT
content-type	text/html
content-length	645
server	nginx/1.21.0
last-modified	Tue, 29 Nov 2022 00:48:40 GMT
etag	"638556e8-285"
x-frame-options	**SAMEORIGIN**
x-content-type-options	**nosniff**
referrer-policy	**strict-origin-when-cross-origin**
permissions-policy	**accelerometer**=(), **camera**=(), **geolocation**=(), **gyroscope**=(), **magnetometer**=(), **microphone**=(), **payment**=(), **usb**=()
strict-transport-security	**max-age**=63072000; **includeSubDomains**; **preload**
accept-ranges	bytes

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 browser from loading malicious assets.

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 COR
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.
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.
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 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.
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.