


Security Headers

Sponsored byProbely

HomeAbd


Scan your site now

https://certvet-front.us-east-1.elasticbear

Scan

☐ Hide results☒ Follow redirects

Security Report Summary



Site:<https://certvet-front.us-east-1.elasticbeanstalk.com/>

IP Address:3.225.18.130

Report Time:28 Nov 2022 23:24:28 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	Mon, 28 Nov 2022 23:24:27 GMT
content-type	text/html
content-length	645
server	nginx/1.21.0
last-modified	Mon, 28 Nov 2022 04:08:19 GMT
etag	"63843433-285"
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.

https://securityheaders.com/?q=https%3A%2F%2Fcertvet-front.us-east-1.elasticbeanstalk.com%2F&followRedirects=on

1/2

Cross-Origin-Resource-Policy	<a href="#">Cross-Origin Resource Policy</a> allows a resource owner to specify who can load the resource.

Additional Information	
server	This <a href="#">Server</a> header seems to advertise the software being run on the server but you can remove or change this value.
x-frame-options	<a href="#">X-Frame-Options</a> 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	<a href="#">X-Content-Type-Options</a> stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. A valid value for this header is "X-Content-Type-Options: nosniff".
referrer-policy	<a href="#">Referrer Policy</a> is a new header that allows a site to control how much information the browser includes with navigations away from a site. It should be set by all sites.
permissions-policy	<a href="#">Permissions Policy</a> is a new header that allows a site to control which features and APIs can be used in the browser.
strict-transport-security	<a href="#">HTTP Strict Transport Security</a> is an excellent feature to support on your site and strengthens your implementation of TLS by getting the browser to enforce the use of HTTPS.

A <a href="#">scotthelme.co.uk</a> project - <a href="#">CC-BY-SA 4.0</a>	Sponsored by <a href="#">Probely</a> .