Scan your site now

https://estagiei.herokuapp.com/api/vaga Scan

Hide results Follow redirects

Security Report Summary

A+

Site:	https://estagiei.herokuapp.com/api/vaga
IP Address:	23.22.130.173
Report Time:	06 Jun 2022 16:15:13 UTC
Headers:	✔ Strict-Transport-Security ✔ Content-Security-Policy ✔ X-Frame-Options ✔ X-Content-Type-Options ✔ Referrer-Policy ✔ Permissions-Policy

Supported By

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

Raw Headers

HTTP/1.1	200
Server	Cowboy
Connection	keep-alive
Accept	application/json
Strict-Transport-Security	**max-age**=63072000; **includeSubDomains**; **preload**
Content-Security-Policy	**default-src** *'self'* https://estagiei.herokuapp.com
X-Frame-Options	**DENY**
X-Content-Type-Options	**nosniff**
Referrer-Policy	**same-origin**
Permissions-Policy	**microphone**=none; **geolocation**=none;**camera**=none
Vary	Origin
Vary	Access-Control-Request-Method
Vary	Access-Control-Request-Headers
Content-Type	application/json
Transfer-Encoding	chunked
Date	Mon, 06 Jun 2022 16:15:13 GMT
Via	1.1 vegur

Upcoming Headers

Expect-CT	Expect-CT allows a site to determine if they are ready for the upcoming Chrome requirements and/or enforce their CT policy.
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".
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.
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.
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.
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.