Security Headers

Sponsored by Report URI

Home About Donate

Scan your site now

camposcasares.be Scan

Hide results Follow redirects

Security Report Summary

A

Site:	https://www.camposcasares.be/
IP Address:	2001:41d0:404:200::31f9
Report Time:	02 Jun 2020 21:47:48 UTC
Headers:	✔ Strict-Transport-Security ✔ X-Content-Type-Options ✔ X-Frame-Options ✔ Content-Security-Policy ✔ Referrer-Policy ✖ Feature-Policy
Warning:	Grade capped at A, please see warnings below.

Supported By

Raw Headers

HTTP/1.1	200 OK
Server	nginx
Date	Tue, 02 Jun 2020 21:47:48 GMT
Content-Type	text/html

Content-Length	6588
Last-Modified	Tue, 02 Jun 2020 13:44:47 GMT
Connection	keep-alive
ETag	"5ed657cf-19bc"
Strict-Transport-Security	**max-age**=31536000; **includeSubDomains**; **preload**
X-XSS-Protection	**1**; **mode**=block
X-Content-Type-Options	**nosniff**
X-Frame-Options	**DENY**
Content-Security-Policy	**frame-src** *'self'* https://www.google.com https://www.gstatic.com https://s74.cwb.ovh; **default-src** *'self'* https://s74.cwb.ovh; **script-src** *'self'* *'unsafe-inline'* https://maxcdn.bootstrapcdn.com https://ajax.googleapis.com https://www.google.com https://www.gstatic.com; **img-src** *'self'*; **style-src** *'self'* *'unsafe-inline'* https://fonts.googleapis.com https://kit-free.fontawesome.com https://maxcdn.bootstrapcdn.com; **font-src** *'self'* data: https://kit-free.fontawesome.com https://fonts.gstatic.com https://maxcdn.bootstrapcdn.com; **form-action** *'self'*; **upgrade-insecure-requests**;
Referrer-Policy	**strict-origin-when-cross-origin**
Accept-Ranges	bytes

Missing Headers

Feature-Policy	Feature Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Warnings

Content-Security-Policy	This policy contains 'unsafe-inline' which is dangerous in the script-src directive. This policy contains 'unsafe-inline' which is dangerous in the style-src directive.

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.

Additional Information

Server	This Server header seems to advertise the software being run on the server but you can remove or change this value.

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.
X-XSS-Protection	X-XSS-Protection sets the configuration for the XSS Auditor built into older browser. The recommended value was "X-XSS-Protection: 1; mode=block" but you should now look at Content Security Policy instead.
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".
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.
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.
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.