Security Headers
by snyk

Scan your site now

https://portfolio.mmi25a01.mmi-troyes.f Scan

Hide results Follow redirects

Security Report Summary

A+

Site:	https://portfolio.mmi25a01.mmi-troyes.fr/
IP Address:	45.147.96.53
Report Time:	25 Jun 2026 19:59:12 UTC
Headers:	✔ X-Content-Type-Options ✔ X-Frame-Options ✔ Referrer-Policy ✔ Permissions-Policy ✔ Content-Security-Policy ✔ Strict-Transport-Security
Advanced:	Wow, amazing grade! Perform a deeper security analysis of your website and APIs: Try Now

Raw Headers

HTTP/1.1	200 OK
Date	Thu, 25 Jun 2026 19:59:12 GMT
Server	Apache/2.4.67 (Debian)
X-Content-Type-Options	**nosniff**
X-Frame-Options	**SAMEORIGIN**
Referrer-Policy	**strict-origin-when-cross-origin**
Permissions-Policy	**camera**=(), **microphone**=(), **geolocation**=()
Content-Security-Policy	**default-src** 'self'; **img-src** 'self' data:; **style-src** 'self'; **script-src** 'self'; **base-uri** 'self'; **form-action** 'self'
Strict-Transport-Security	**max-age**=31536000; **includeSubDomains**
Set-Cookie	PHPSESSID=blfq3ltapfmpkfod14s0l1cokj; path=/; **secure**; **HttpOnly**; **SameSite**=Strict
Expires	Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control	no-store, no-cache, must-revalidate
Pragma	no-cache
Vary	Accept-Encoding
Content-Encoding	gzip
Content-Length	5448
Content-Type	text/html; charset=UTF-8

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

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.
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.
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.
Set-Cookie	There is no Cookie Prefix on this cookie.