Security Headers by snyk

Home About API

Digitally signed by LUBOMIR GEORGIEFF MEGOFF
Date: 2026.01.12 20:39:21 +02'00'

Scan your site now

www.computeon.house

Scan

Hide results Follow redirects

Security Report Summary

A+

Site:	https://www.computeon.house/
IP Address:	185.199.38.4
Report Time:	22 Dec 2025 11:09:45 UTC
Headers:	✔ Strict-Transport-Security ✔ Content-Security-Policy ✔ X-Content-Type-Options ✔ Referrer-Policy ✔ Permissions-Policy ✔ X-Frame-Options
Advanced:	Wow, amazing grade! Perform a deeper security analysis of your website and APIs: Try Now

Raw Headers

HTTP/2	200
content-type	text/html

last-modified	Mon, 22 Dec 2025 10:49:37 GMT
accept-ranges	bytes
content-encoding	gzip
vary	Accept-Encoding
content-length	1637
date	Mon, 22 Dec 2025 11:09:45 GMT
server	LiteSpeed
strict-transport-security	**max-age**=31536000; **includeSubDomains**; **preload**
content-security-policy	**upgrade-insecure-requests**; **default-src** 'self'; **base-uri** 'none'; **object-src** 'none'; **frame-ancestors** 'self'; **script-src** 'self'; **style-src** 'self'; **img-src** 'self' data:; **font-src** 'self'; **connect-src** 'self'; **report-uri** /csp-report
x-content-type-options	**nosniff**
referrer-policy	**strict-origin-when-cross-origin**
permissions-policy	**camera**=(), **microphone**=(), **geolocation**=(), **usb**=(), **payment**=(), **accelerometer**=(), **gyroscope**=(), **magnetometer**=(), **fullscreen**=(self)
cross-origin-resource-policy	**same-origin**
cross-origin-embedder-policy	**require-corp**
cross-origin-opener-policy	**same-origin**
x-frame-options	**DENY**
link	</.well-known/security.txt>; rel=security
alt-svc	h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

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-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.
cross-origin-resource-policy	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.
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.
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.

A snyk.io project - CC-BY-SA 4.0 Powered by Snyk