

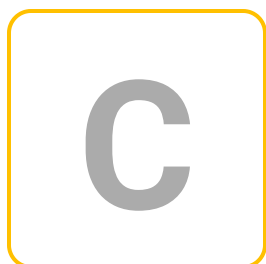
Scan your site now

eciru.i

Scan

☐ Hide results ☒ Follow redirects

Security Report Summary



Site: <https://eciru.ir/>

IP Address: 185.211.59.237

Report Time: 04 Jul 2025 12:51:51 UTC

Headers: ☒ X-Content-Type-Options ☒ Referrer-Policy ☒ Content-Security-Policy
☒ Strict-Transport-Security ☒ X-Frame-Options ☒ Permissions-Policy

Not bad... Maybe you should perform a deeper security analysis of your website and APIs:

Advanced:

[Try Now](#)

Using Headers

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. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".

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. Recommended value "X-Frame-Options: SAMEORIGIN".

Permissions-Policy

[Permissions Policy](#) is a new header that allows a site to control which features and APIs can be used in the browser.

Raw Headers

HTTP/1.1	200 OK
Date	Fri, 04 Jul 2025 12:51:46 GMT
Server	Apache
X-XSS-Protection	0
X-Content-Type-Options	nosniff
Referrer-Policy	strict-origin-when-cross-origin
Content-Security-Policy	upgrade-insecure-requests;
Link	<https://eciru.ir/wp-json/;> rel="https://api.w.org/", <https://eciru.ir/wp-json/wp/v2/pages/6>; rel="alternate"; title="JSON"; type="application/json", <https://eciru.ir/;> rel=shortlink
Vary	Accept-Encoding,User-Agent
Content-Encoding	gzip
Content-Length	38541
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-XSS-Protection

[X-XSS-Protection](#) sets the configuration for the XSS Auditor built into older browsers. 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".

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.

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.

A [snyk.io](#) project - [CC-BY-SA 4.0](#)

Powered by [Snyk](#)

