Security Headers

by Probely, a snyk Business

Scan your site now

files.liquidfiles.com

Scan

Hide results Follow redirects

Security Report Summary

A+

Site:	https://files.liquidfiles.com/
IP Address:	44.219.36.83
Report Time:	12 Dec 2024 01:18:27 UTC
Headers:	✔ X-Frame-Options ✔ X-Content-Type-Options ✔ Referrer-Policy ✔ Strict-Transport-Security ✔ Permissions-Policy ✔ Content-Security-Policy
Advanced:	Wow, amazing grade! Perform a deeper security analysis of your website and APIs: Try Now

Raw Headers

HTTP/2	200
date	Thu, 12 Dec 2024 01:18:27 GMT
content-type	text/html; charset=utf-8
vary	Accept-Encoding
x-frame-options	**SAMEORIGIN**
x-content-type-options	**nosniff**
x-download-options	noopen
x-permitted-cross-domain-policies	none
referrer-policy	**strict-origin-when-cross-origin**
x-robots-tag	noindex, nofollow
x-ua-compatible	IE=Edge,chrome=1
strict-transport-security	**max-age**=63072000
permissions-policy	**camera**=(), **gyroscope**=(), **microphone**=(), **usb**=(), **payment**=(), **geolocation**=(), **fullscreen**=(self) **geolocation**=(self)
cache-control	max-age=86400, public
pragma	no-cache
expires	Mon, 01 Jan 1990 00:00:00 GMT
x-forwarded-for	undefined
link	</assets/application-6ad41b9200658052f845115566cc28480bef6767fc75b28ba1086a39c61b952a.css>; rel=preload; as=style; nopush,</i18n/en-3ca4e0f83dd17cfeb9194bd731bafa9ea5102efee117866ac3d3588af8e08220.js>; rel=preload; as=script; nopush,</assets/application-8b156d18cab54c-cbb1ad0110a45fecdde0260d2b843601daf8613e6fde4f8329.js>; rel=preload; as=script; nopush
vary	Accept
content-security-policy	**default-src** 'none'; **base-uri** 'none'; **frame-ancestors** 'none'; **img-src** 'self'; **script-src** 'strict-dynamic' 'nonce-pXD98kHj5StixVU/CroDlg=='; **style-src** 'self' 'nonce-pXD98kHj5StixVU/CroDlg==' 'sha256-J7S43U7P4IyRwR2p1HK6h8nBUj1WYn8uQhCoaTy1GMU=' ; **font-src** 'self'; **connect-src** 'self';
etag	W/"79370febfc0a62d14148df3ef934476b"
feature-policy	**accelerometer** 'none'; **ambient-light-sensor** 'none'; **autoplay** 'none'; **camera** 'none'; **encrypted-media** 'none'; **fullscreen** 'self'; **geolocation** 'none'; **gyroscope** 'none'; **magnetometer** 'none'; **microphone** 'none'; **midi** 'none'; **payment** 'none'; **picture-in-picture** 'none'; **speaker** 'none'; **usb** 'none'; **vibrate** 'none'; **vr** 'none'
set-cookie	_filetransfer_session=GJA1ZBMNZnUoBPPmqdpCJuZsmWjowcwjd1PONMoT6YQdKmYWc3T2A2%2B0ZGOSNoBTvQwa6nykQWFwxT17wfrZvh7ScAgjqv-ZGc1I3Yj2pHKpNRq3tN9wD9mF3t6CxvdJO5VFLk1kr0mxOk7%2B%2F6N0W1JkjIa%2Fs8sshOtGQMhRKnAQvxNQWBXPEyFLNgD4Q7vNf0l-VBF%2B7ZW99RaN19dtlEvnGVG45ChZ73gD6DSjZm4dvdxzuKIrXhop9ebG5xVEMkJQ%2B99kYSvr%2BpDDYIR78EcjPAx6kHNK3RskaLe2I%3D--1vH9Qov-QwPutpuEC--E2iPHSBMgABDU%2BgFum%2FW2Q%3D%3D; path=/; **secure**; **HttpOnly**; **SameSite**=Lax
x-request-id	e644f9ec-bcf3-4ef3-85fe-2434498636c5
content-encoding	gzip

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

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.
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.
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.
feature-policy	Feature Policy has been renamed to Permissions Policy, see the details here.
set-cookie	There is no Cookie Prefix on this cookie.