Security Headers
Sponsored by Probely

Home About Donate

Scan your site now

gettr.com | **Scan**

☑ Hide results ☑ Follow redirects

Security Report Summary

F

Site:	https://gettr.com/
IP Address:	2600:9000:234b:3200:1a:d6d6:9e80:93a1
Report Time:	06 Jan 2022 17:12:33 UTC
Headers:	✖ Strict-Transport-Security ✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy

Supported By

Probely	Ouch, you should work on your security posture immediately: **Start Now**

Raw Headers

HTTP/2	200
content-type	text/html

content-length	5555
last-modified	Thu, 06 Jan 2022 02:54:27 GMT
accept-ranges	bytes
server	AmazonS3
date	Thu, 06 Jan 2022 17:12:34 GMT
cache-control	max-age=0,no-cache,no-store,must-revalidate
etag	"46e53eccfcad827c7fb9cf73817e1f0b"
x-cache	Error from cloudfront
via	1.1 7256fedee68a59a508800e0dda035348.cloudfront.net (CloudFront)
x-amz-cf-pop	SFO5-P2
x-amz-cf-id	PIV2fF2NsupLU59WvbfiKYNonvU1yB97OQzFtM8H7kxojLy0UCzhzQ==

Missing 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".
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.
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".
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.

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.
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.

A scotthelme.co.uk project - CC-BY-SA 4.0

Sponsored by Probely