Security headers

Header	What it does	Safe starting value	Watch out for
Strict-Transport-Security	Tells browsers to use HTTPS only for this host	`max-age=31536000; includeSubDomains`	Only add `preload` once every subdomain serves HTTPS
Content-Security-Policy	Limits where scripts, styles and frames may load from	Start with `Content-Security-Policy-Report-Only` and a `default-src 'self'` policy	Inline scripts and third-party widgets break until they're allowed
X-Frame-Options	Stops other sites framing your pages (clickjacking)	`SAMEORIGIN`	Being replaced by CSP `frame-ancestors`; send both for older browsers
X-Content-Type-Options	Stops MIME-type sniffing	`nosniff`	Files served with the wrong Content-Type stop working
Referrer-Policy	Controls how much of the URL is sent as Referer	`strict-origin-when-cross-origin`	`no-referrer` can break analytics attribution
Permissions-Policy	Turns off browser features you don't use	`camera=(), microphone=(), geolocation=()`	Don't block a feature a page actually needs

Check headers after every server or CDN change. A rewrite rule or proxy can quietly drop them. Test the final URL after redirects, not just the bare domain.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com