
Content-Security-Policy	default-src 'self'	Limit where content can load from
X-Content-Type-Options	nosniff	Disable MIME sniffing
Strict-Transport-Security	max-age=31536000; includeSubDomains	Force HTTPS
Referrer-Policy	strict-origin-when-cross-origin	Limit referrer data
Permissions-Policy	camera=(), microphone=()	Disable browser features
X-Frame-Options	DENY	Prevent clickjacking (or CSP frame-ancestors)
Cross-Origin-Opener-Policy	same-origin	Isolate browsing context