HTTP Security Headers Matrix

HTTP Security headers per URL.

CORS (Cross Origin Resource Sharing)

Tell a browser to let a web application running at one origin (domain) have permission to access selected resources from a server at a different origin

CSP (Content Security Policy)

Mitigate and report cross site scripting attacks by telling the browser what it should and shouldn't load and execute.

Expect-CT (Expect Certificate Transparancy)

Opt in to reporting and/or enforcement of Certificate Transparency requirements, which prevents the use of misissued certificates for that site from going unnoticed.

Feature Policy

Instruct the browser about which browser features (camera, geolocation, fullscreen, etc) the web application is allowed to use.

HPKP (HTTP Public Key Pinning)

A security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

Referrer Policy

Instruct the browser on which information to include in the Referrer header on subsequent requests.

HSTS (Strict Transport Securiy)

Tell the user's browser to always connect to the HTTPS version of the site from now on, and skip redirects from a non-secure (http) version of the site.

Content-type options

Instruct the browser not to guess the content type of data, but to trust the server's indication of the content type.

Frame Options

Tell the browser whether the current site may be loaded in a frame or iframe.

XSS Protection

Instruct old browsers to activate their Cross site scripting protection.

	CORS Headers	CORS Methods	CORS Origin	CSP	Except CT	Feature Policy	HPKP	Referrer Policy	HTST	Content-type options	Frame Options	XSS Protection
https://github.com/	None	None	None	default-src 'none'; base-uri 'self'; block-all-mixed-content; connect-src 'self' uploads.github.com www.githubstatus.com collector.githubapp.com api.github.com www.google-analytics.com github-cloud.s3.amazonaws.com github-production-repository-file-5c1aeb.s3.amazonaws.com github-production-upload-manifest-file-7fdce7.s3.amazonaws.com github-production-user-asset-6210df.s3.amazonaws.com wss://live.github.com; font-src github.githubassets.com; form-action 'self' github.com gist.github.com; frame-ancestors 'none'; frame-src	max-age=2592000, report-uri="https://api.github.com/_private/browser/errors"	None	None	origin-when-cross-origin, strict-origin-when-cross-origin	max-age=31536000; includeSubdomains; preload	nosniff	deny	1; mode=block

				render.githubusercontent.com; img-src 'self' data: github.githubassets.com identicons.github.com collector.githubapp.com github-cloud.s3.amazonaws.com *.githubusercontent.com customer-stories-feed.github.com; manifest-src 'self'; media-src 'none'; script-src github.githubassets.com; style-src 'unsafe-inline' github.githubassets.com									
https://gitlab.com/	None	None	None	frame-ancestors 'self' https://gitlab.lookbookhq.com https://learn.gitlab.com;	None		None	None	None	max-age=31536000; includeSubdomains	nosniff	None	1; mode=block