HTTP Security Headers

No	Name	Description	Policies	Attacks
1	**X-Content-Type-Options**	MIME sniffing attacks prevention	nosniff -> Blocks a request if the request destination is of type style and the MIME type is not text/css, or of type script	Misconfigure RFD
2	**X-XSS-Protection**	Detect reflected cross-site scripting	0 -> Allow 1 -> Enables XSS filtering mode=block -> browser will prevent rendering of the page if an attack is detected. report=<reporting-URI> -> sanitize the page and report the violation	Misconfigure CORS Deception
3	**X-Frame-Options**	Browser should be allowed to render a page	DENY -> deny displayed in a frame SAMEORIGIN -> displayed if all ancestor frames are same origin to the page itself	Misconfigure Clickjacking
4	**Content-Security-Policy**	Control what resources	default-src -> come from the site's own origin media-src -> media to trusted providers script-src -> specific server that hosts trusted code	Misconfigure XSS Clickjacking
5	**Strict-Transport-Security**	informs browsers that the site should only be accessed using HTTPS	max-age -> The time, in seconds, that the browser should remember that a site is only to be accessed using HTTPS. includeSubDomains -> rule applies to all of the site's subdomains as well	Misconfigure MITM SSL/TLS Stripping attacks Cookie hijacking attacks
6	**Referrer-Policy**	sent requests do not include any referrer information	no-referrer -> not include any referrer information no-referrer-when-downgrade -> Don't send the Referer header for requests to less secure destinations (HTTPS→HTTP, HTTPS→file)	Misconfigure CSRF Privacy attacks Information disclosure attacks

Virtual Patching Heatmap

Attacks Heatmap

HTTP Security Headers

No	Name	Description	Policies	Attacks
7	**Cache-Control**	control caching in browsers and shared caches	no-cache -> response must be validated with the origin server before each reuse no-store -> response directive indicates that any caches of any kind (private or shared) should not store this response.	Misconfigure Cache Inspection Cache Deception
8	**Content-Disposition**	response header is a header indicating if the content is expected to be displayed inline in the browser	inline attachment filename="filename.jpg"	Misconfigure XSS clickjacking RFD
9	**Cross-Origin-Resource-Policy**	protection against certain requests from other origins	same-site -> Only requests from the same Site can read the resource. same-origin -> requests from the same origin (i.e. scheme + host + port) cross-origin -> any origin (both same-site and cross-site) can read the resource	Misconfigure XSS clickjacking
10	**X-***	Extra HTTP Header	X-Rate-Limit: Control Limit of request X-Origin -> Origin of requests X-Forwarded-IP -> Change Real IP	Misconfigure Http Header Injection Cache Deception Ratelimit Bypass
11	**Content-Encoding**	lists any encodings that have been applied to the representation (message payload), and in what order	gzip compress deflate br	DDoS Network eavesdropping
12	**Access-Control-Allow-Origin**	whether the response can be shared with requesting code from the given origin	* <origin> null	Misconfigure XSS Host Header Injection Cache Poisoning
13	**Access-Control-Allow-Methods**	specifies one or more methods allowed	POST, GET, OPTIONS *	Misconfigure CSRF XSS

Virtual Patching Heatmap

Attacks Heatmap