Security Headers Implementation

After a comprehensive study about security headers the following are the one which sound important.

Content Security Policy (CSP): is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross-Site Scripting and data injection attacks. These attacks are used for everything from data-theft to site defacement, to malware distribution.

HTTP Strict Transport Security (HSTS): Prevents any attempt to connect to your site over plain HTTP. Helps stop man-in-the-middle attacks and upgrades your site’s security. Also highly recommended.

X-Frame Options: can be used to indicate whether a browser should be allowed to render a page in a <frame>, <iframe>, <embed> or <object>. Sites can use this to avoid click-jacking attacks, by ensuring that their content is not embedded into other sites.

X-XSS-Protection: Prevents some forms of cross site scripting attack, by preventing script from executing if any of the markup in the document is also present in the same form in the request.

X-Content-Type-Options: Set this to no sniff to prevent browsers allowing content that looks like JavaScript to execute even if it doesn’t have the right content-type. Prevents mime confusion attacks, and more recently is being used by Chrome to enable site isolation. It’s getting less necessary over time, due to better default behaviours, but this is currently still a best practice.

Cross-Origin-Resource-Sharing: Cross-Origin Resource Sharing headers allow your URL to be loaded by script operating on another origin. This one's optional. These headers are permissive, not restrictive, so not having them at all gives you the highest level of security.

Referrer-Policy: Configures the level of detail to include in the Referrer header when navigating away from the page. Helps to prevent data leaking from your site to sites that you link to. Highly recommended.