Configure HTTP Headers

Scan your installation using .

There are a number of headers which we suggest to enable:

- X-Frame-Options: SAMEORIGIN
  tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking.
- X-Content-Type-Options: nosniff
  stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type.
- X-XSS-Protection: 1; mode=block
  sets the configuration for the XSS Auditor built into older browsers.
- Referrer-Policy: strict-origin-when-cross-origin
  is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
- Strict-Transport-Security: max-age=31536000
  should be used after enabling SSL. It strengthens the implementation of TLS by getting the User Agent to enforce the use of HTTPS.
- Content-Security-Policy: upgrade-insecure-requests
  is a new method of enforcing what a user agent can load on a given page. It supersedes X-Frame-Options, X-Content-Type-Options, X-XSS-Protection in modern browsers. All content loaded by SupportPro is served from your servers so the majority of policy directives should be set to self. script-src and style-src need to permit unsafe-inline as

at this time our templates have a lot of inline JavaScript and CSS without nonces.

Please consult your web server documentation for steps on how to configure these headers.