## Missing HTTP Security Headers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Category | Protection Mechanism Failure [CWE-693] | | | |
| Status | Open | | | |
| Impact | Minor | | | |
| Likelihood | Very Unlikely | | | |
| Risk | Information | | | |

HTTP Security headers are a method of improving the default level of security offered by a web browser. Thereby lack of a security header does not constitute a vulnerability itself but is considered lack of hardening. It is recommended that all available headers be reviewed and where possible implemented.

The following headers were either missing or not set to a recommended value:

|  |  |
| --- | --- |
| Header | Description |
| Strict Transport Security | Strict Transport Security enforces the use of HTTPS in the web browser, ensuring that no information is sent for the domain (and optionally subdomains too), even if a link to a plain HTTP page is included or the user unintentionally navigates to a HTTP link. This additionally mitigates the risk of cookies without the secure flag set, by enforcing HTTPS only. |
| Content Security Policy | Content Security Policy allows you to whitelist web application resource locations, including where scripts can be loaded from and where the application may be framed. This can therefore mitigate reflected cross-site scripting attacks as well as issues such as Clickjacking. |
| X-Content-Type-Options | X-Content-Type-Options prevents a browser from attempting to enumerate the MIME-type of a server response, thereby preventing some types of cross-site scripting attack. |
| Referrer Policy | Referrer Policy allows a web application to reduce when the “referrer” header is set. Thereby preventing sensitive data in the URL from being transmitted to third-parties or over insecure connections. |
| X-Frame-Options | X-Frame-Options is one method of controlling which sites may frame the web application, however it is not fully implemented in Chrome (in favour of CSP). Thereby the only available options are DENY or SAMEORIGIN. If more granularity is required, consider CSP instead. Preventing framing can prevent Clickjacking attacks. |