## 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, incorrect or not set to a recommended value:

|  |  |
| --- | --- |
| Header | Description |

## Incorrectly configured cookies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Category | Protection Mechanism Failure [CWE-693] | | | |
| Status | Open | | | |
| Impact | Minor | | | |
| Likelihood | Likely | | | |
| Risk | Low | | | |

Cookie configuration via both security and non-security focused cookie attributes can greatly improves site security. This is achieved by preventing disclosure of information and by reducing the attack surface making exploitation of other vulnerabilities significantly harder. It is recommended that all cookies on the specified pages be reviewed taking into consideration the missing or incorrectly set cookie attributes highlighted in the table below.

|  |  |
| --- | --- |
| Cookie Attribute | Description/Issue |