

**Finding Name:** Strict-Transport-Security (HSTS) Missing Header

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Poorna Dabare | PT | Senior Team Member | Ontrack |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

The absence of the Strict-Transport-Security (HSTS) header allows for the possibility of man-in-the-middle attacks, where a malicious actor can intercept or alter communications between the user and the application.

**Risk Rating**  
Impact: Significant  
Likelihood: Moderate

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

Not having an HSTS header may lead to communication being compromised, which can result in loss of customer trust, theft of sensitive information, and potential legal consequences. Ensuring HSTS is implemented would help protect user data and uphold the integrity and reputation of OnTrack.

**Affected Assets**

* OnTrack Web Application
* User Data and Privacy

**Evidence**

Observed and documented that the HSTS header was missing in the security headers list, indicating that the website does not enforce a strict security policy for transport layer protection.

**Steps:**

* Accessed the OnTrack web interface via a secure connection (HTTPS) on a local test server.
* Opened the browser's developer tools to the "Network" tab to monitor the requests and responses.
* Inspected the HTTP response headers for secure requests.

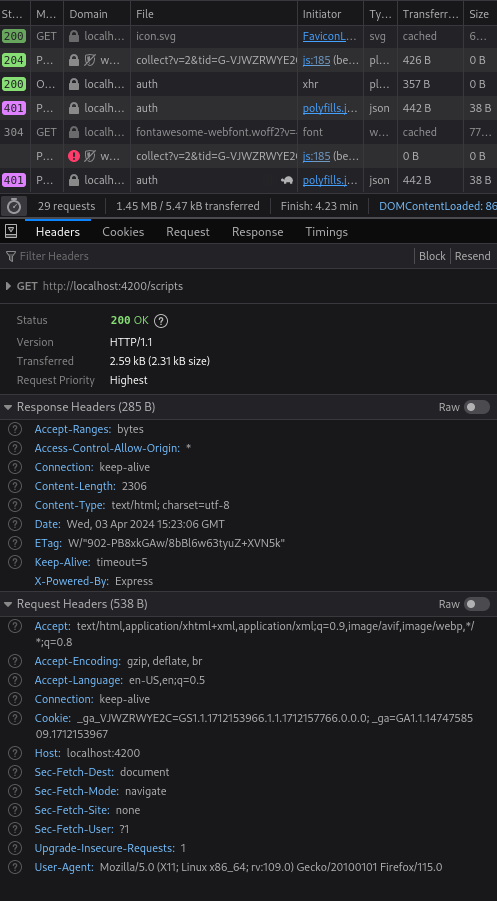


Figure 1

**Remediation Advice**

Implement the Strict-Transport-Security header with an appropriate max-age directive that forces browsers to only use HTTPS, regardless of how the user entered the site URL. This helps in protecting the data from being transmitted over an unencrypted connection.

**References**

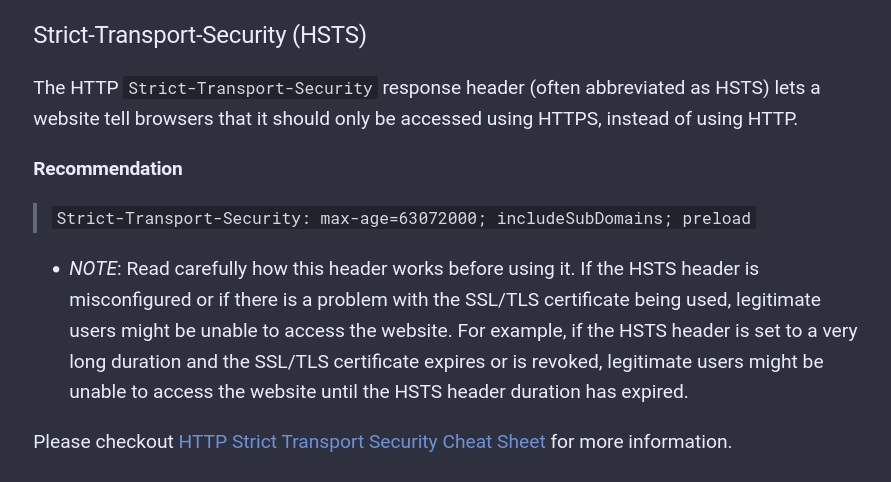
****

Figure 2

[**https://cheatsheetseries.owasp.org/cheatsheets/HTTP\_Headers\_Cheat\_Sheet.html**](https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html)

**Contact Details**

Name: Poorna Dabare

Teams Account: Pen Tester

Email: [s222431648@deakin.edu.au](mailto:s222431648@deakin.edu.au)

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.