

**Finding Name:** Content-Security-Policy (CSP) 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 Content-Security-Policy (CSP) header exposes the OnTrack system to various types of attacks, including Cross-Site Scripting (XSS) and data injection attacks. These vulnerabilities can lead to unauthorized access to user data and the manipulation of web pages to collect information fraudulently.

**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**

Without a CSP, OnTrack's web application lacks an effective control against content injection attacks. This oversight could lead to significant security breaches, undermining user trust and potentially causing legal and financial repercussions for the company. Implementing CSP is crucial for safeguarding against content injection threats, maintaining data integrity, and protecting the company's reputation.

**Affected Assets**

* OnTrack Web Application
* User Data and Privacy

**Evidence**

* Identified that the Content-Security-Policy (CSP) header, which helps safeguard against complex XSS (Cross-Site Scripting) attacks, is not present. This makes the application vulnerable to such security threats.
* Additionally, the X-XSS-Protection header, a security feature that provides a layer of XSS defense for older web browsers, is also missing. This absence further exposes the system, as older browsers might not have adequate protection against XSS without this header.

**Steps:**

* Accessed the OnTrack web application's sign-in page through a local development server (localhost).
* Opened the web browser's developer tools (F12 or right-click > "Inspect") and selected the "Network" tab.
* Performed a page reload while the Network tab was open to capture the incoming and outgoing HTTP requests and responses.
* Searched through the list of assets loaded by the sign-in page to examine the HTTP response headers.

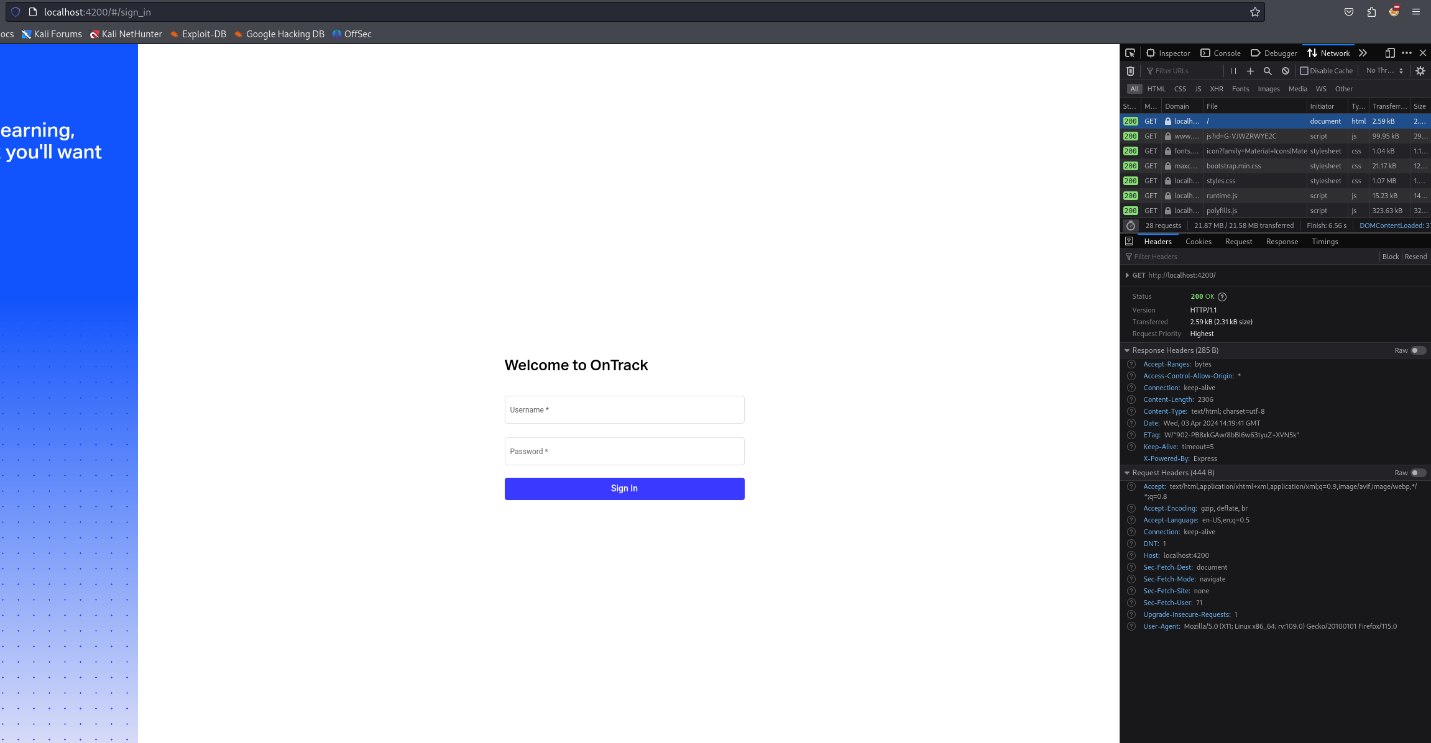
****

Figure 1

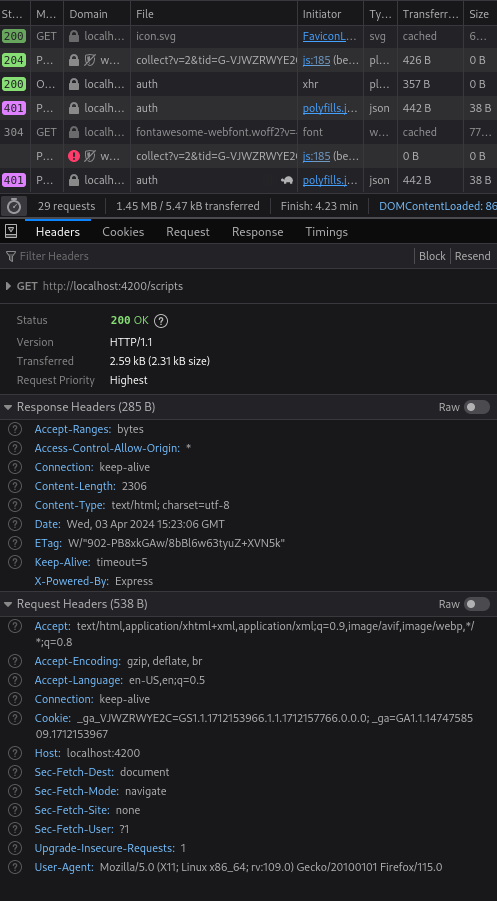


Figure 2

**Remediation Advice**

To mitigate this vulnerability, it is recommended to implement a Content-Security-Policy header with strict rules that only allow scripts, styles, and other resources from trusted sources. Begin by using a restrictive policy and gradually loosen it as necessary, ensuring that only essential resources are permitted. Testing the policy in report-only mode can help identify and adjust the necessary sources without impacting the application's functionality.

**References**

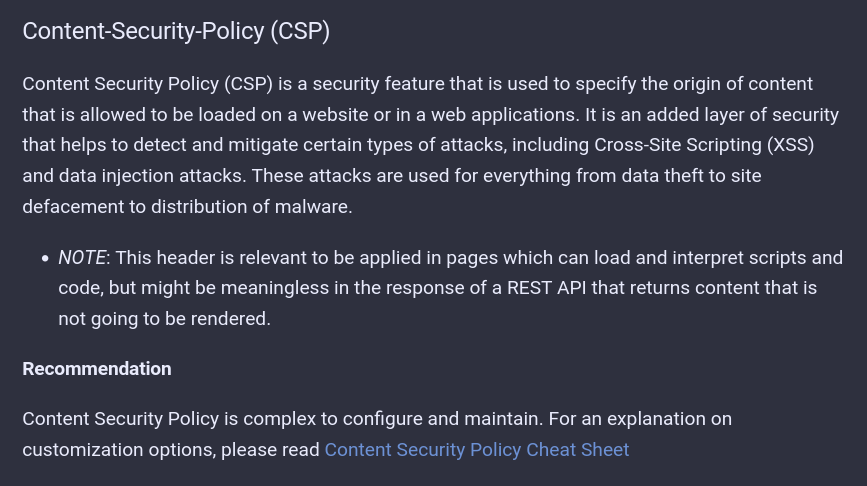
****

Figure 3

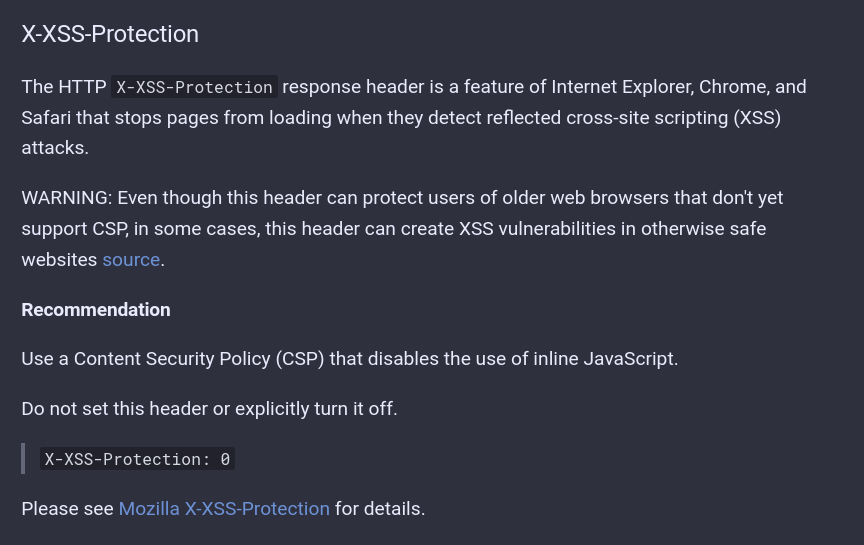


Figure 4

[**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.