

**Finding Name:** **MIME CONFUSION VULNERABILITY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Allen George Thekkemuriyil | PT | Project Member | Ontrack | Nabiha Masood |  |
|  |  |  |  |  |  |

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

**Finding Description:**

The MIME confusion Vulnerability discovered in the localhost:4200 environment involves an issue where the X-Content type-options header is not set to nosniff, but the content-Type header is set to text/html. This configuration creates a vulnerability where browser may interpret the content as HTML and execute malicious scripts.

**Risk Rating**: 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**

The MIME confusion vulnerability poses significant business risks, including potential unauthorized access to sensitive information or execution of malicious scripts. This could result in the legal lilabilities and increased operational costs.

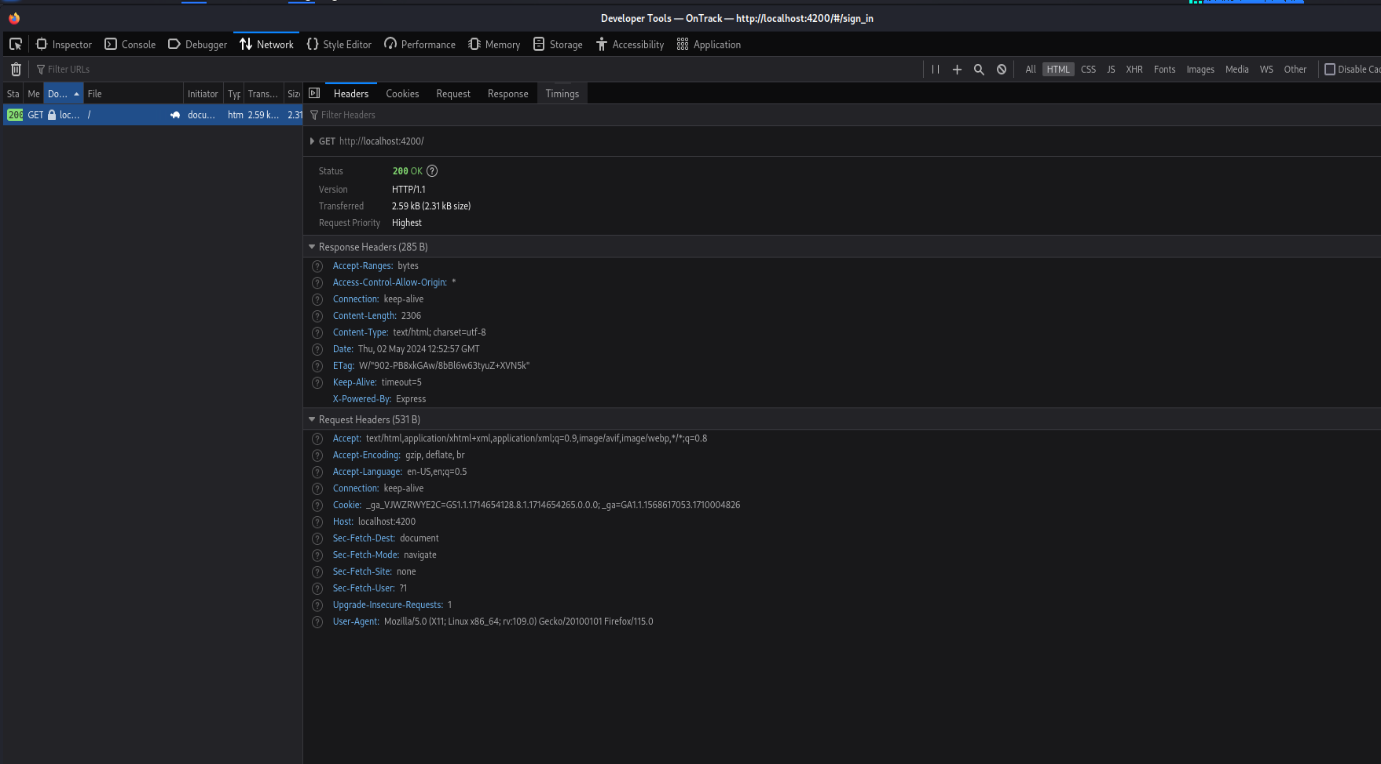
**Affected Assets:**

The vulnerability involves the handling of MIME types within the application. MIME types specify the type and format of data being transmitted over the internet, such as text/html for HTML documents or image/jpeg for JPEG images. The vulnerability may relate to how the application interprets and processes incoming files or content based on their MIME types. This includes parsing files, rendering content, or executing scripts based on MIME type declarations. The vulnerability can be exploited by crafting malicious files with deceptive MIME type declarations to bypass security controls or execute arbitrary code on the server.

**Evidence:**

Step 1:

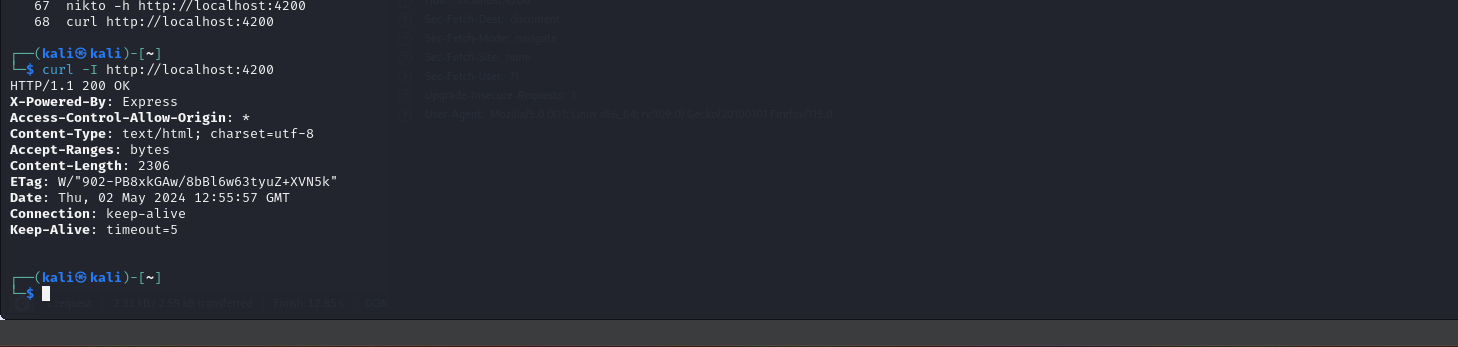
Go to the browser and load the <http://localhost:4200> and using the web developer tools check the network section.



The content type shows the text/html.

Step 2:

In the terminal using curl command and send HTTP requests and displays the response received.



Remediation Advice:

**Content-Type Header Validation:** Implement strict validation of Content-Type header in incoming requests. Ensure only expected and safe Content-Type values are accepted and reject requests with unexpected MIME types. This will prevent MIME confusion vulnerabilities.

**Strict MIME Type Handling:** Configure server to explicitly set the Content-Type header for all HTTP responses. Avoid relying on MIME type detection as it can lead to MIME.

**X-content-Type-Options Header:** Include the X-Content-Type-Options header with the value **nosniff** in HTTP responses. Setting this header will tell the browser not to interpret the content-type header of a response as something other what is specified. Which wll prevent MIME Type sniffing.

Contact:

ALLEN GEORGE THEKKEMURIYIL- [s223027713@deakin.edu.au](mailto:s223027713@deakin.edu.au)

Pentest Leader Feedback: