

**Finding Name:** Information Exposure Through Comments

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Harpreet Singh | PT | Junior Team Member | Ontrack | Oliver Power |  |
|  |  |  |  |  |  |

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

**Finding Description:** While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

**Risk Rating**  
Impact: Major  
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**

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

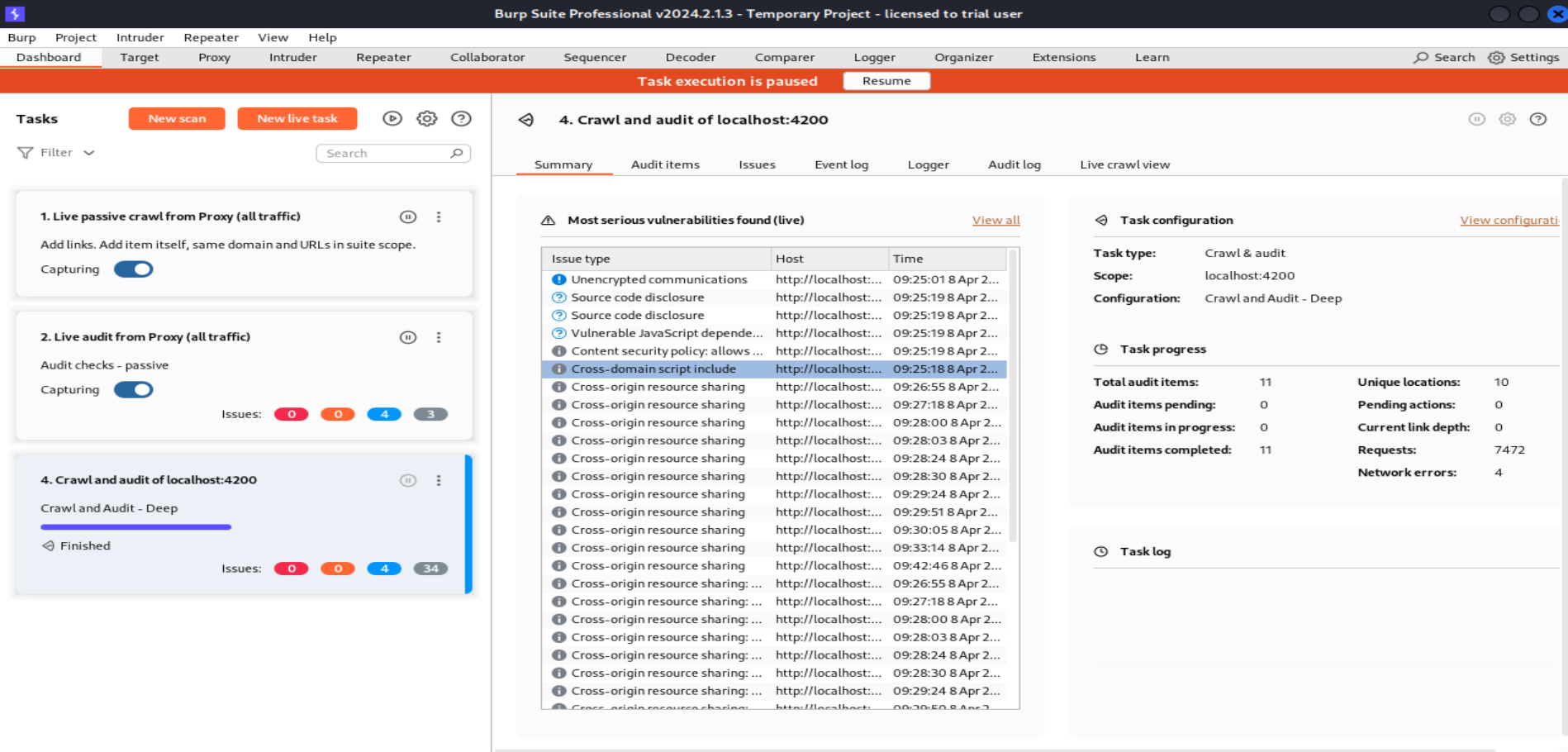
**Affected Assets**

Unauthorized access to sensitive data stored at server side.

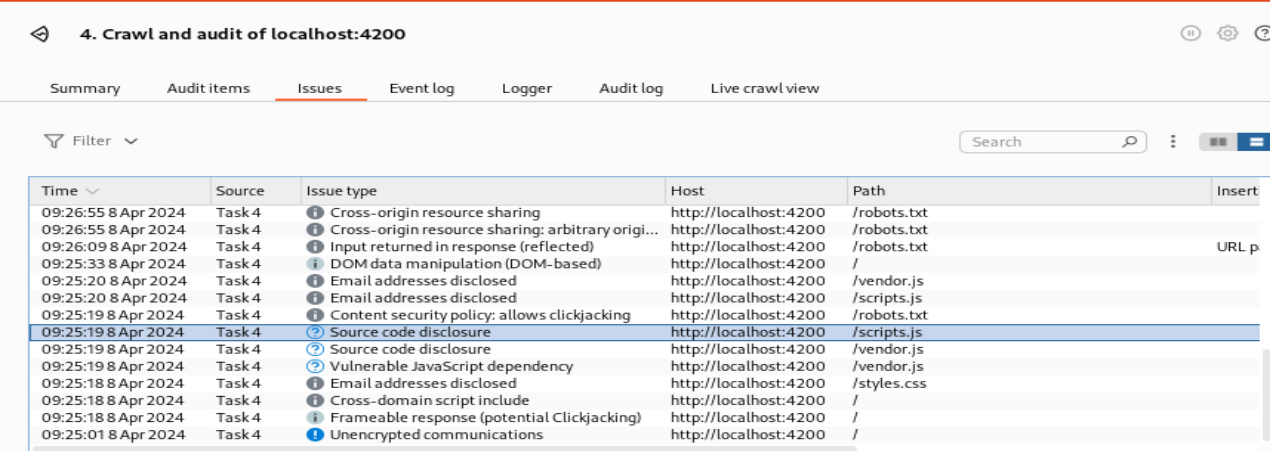
**Evidence**

Provide a step-by-step guide on how to reproduce the vulnerability with screenshots

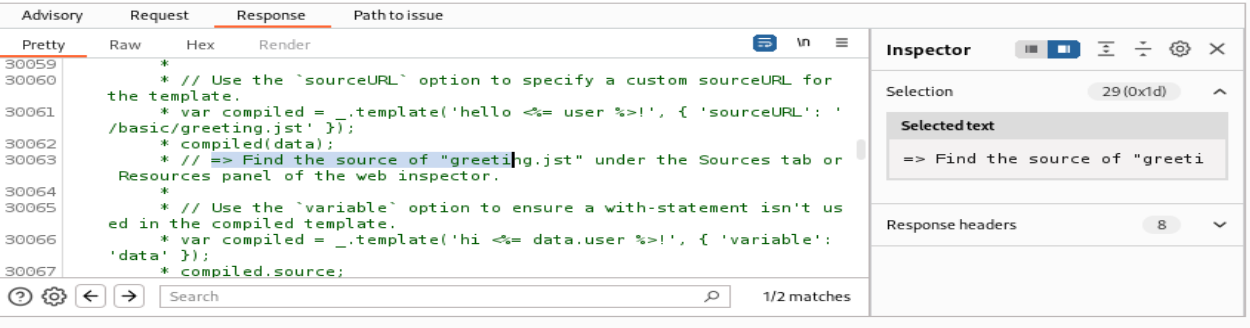
**Step 1. Use new scan from Burp suite to scan the ‘http://localhost:4200/’**



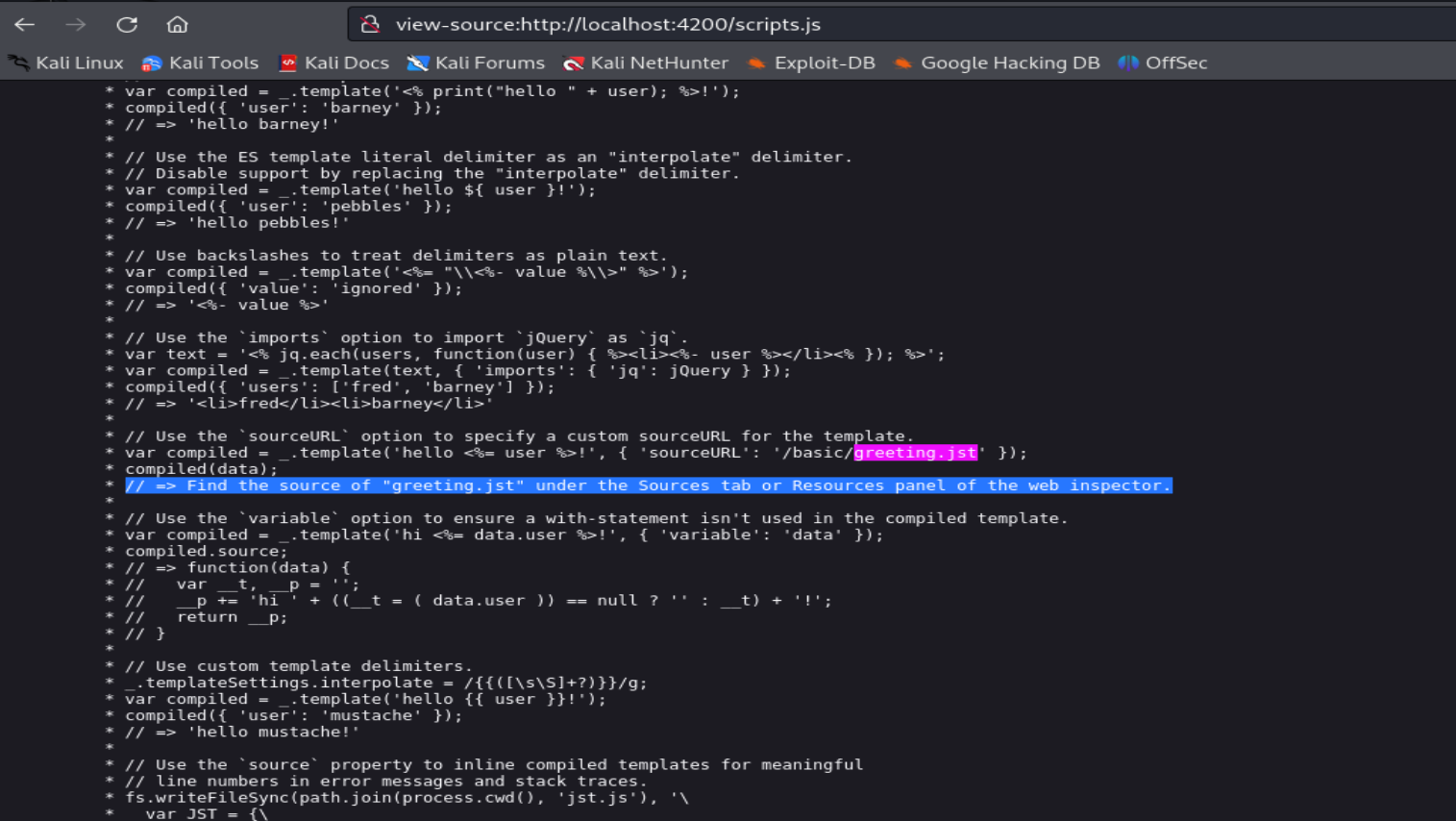
**Step 2. Select the tab ‘Issues’ and find the vulnerability.**



**Step 3. Click on ‘Response’ tab and look for the highlighted comment.**



**Step 4. To verify this found vulnerability, go to ‘view-source:http://localhost:4200/scripts.js’ and search for the above highlighted comment.**



**Remediation Advice**

Remove comments which have sensitive information about the design/implementation of the application. Some of the comments may be exposed to the user and affect the security posture of the application.

**References**

[**https://cwe.mitre.org/data/definitions/615.html**](https://cwe.mitre.org/data/definitions/615.html)

[CWE-615: Information Exposure Through Comments](https://cwe.mitre.org/data/definitions/615.html)

**Contact Details**

Harpreet Singh (singhharpr@deakin.edu.au)

**Pentest Leader Feedback.**