

**Finding Name: Open Redirect Vulnerability**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Jaspriya Kaur | SCR | Senior Lead | Ontrack |  |  |
|  |  |  |  |  |  |

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

**Finding Description**

The vulnerability in sign-in.component.ts at line 116 exposes potential unauthorized access due to inadequate authentication token handling. This oversight could compromise user credentials, posing a significant security risk to the application.

**Risk Rating**

Impact: Major

Likelihood: Unlikely

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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**

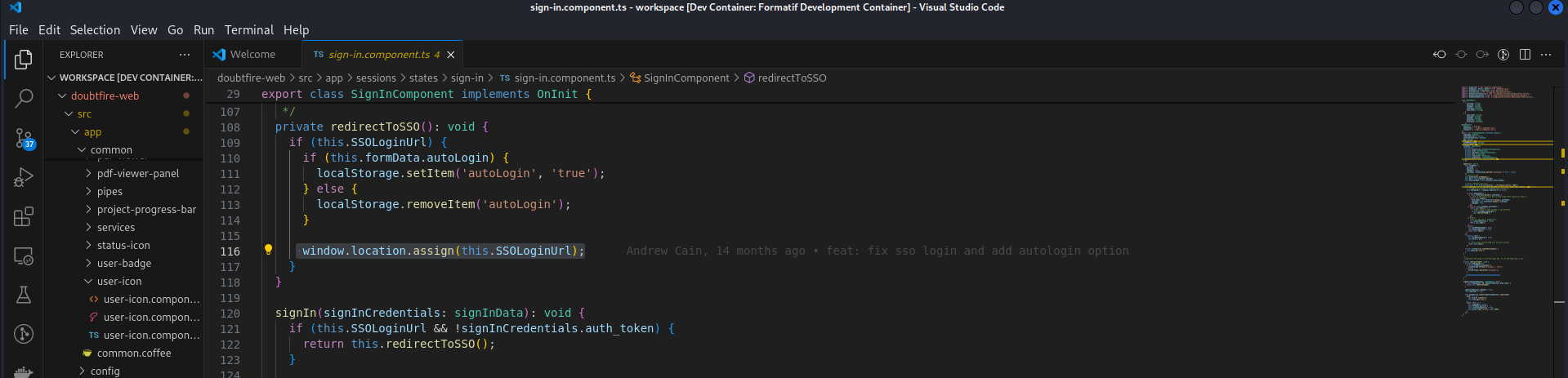
This vulnerability poses a major risk, potentially impacting the regular activity of the application. The affected assets include user authentication and potentially sensitive data.

**Affected Assets**

The vulnerability identified in the `sign-in.component.ts` file at line 116 impacts critical assets related to user authentication and access control within the application. These assets include user credentials, authentication tokens, and potentially sensitive user information stored or processed during the sign-in process. Failure to remediate this vulnerability could result in unauthorized access to user accounts, compromising the integrity and confidentiality of user data.

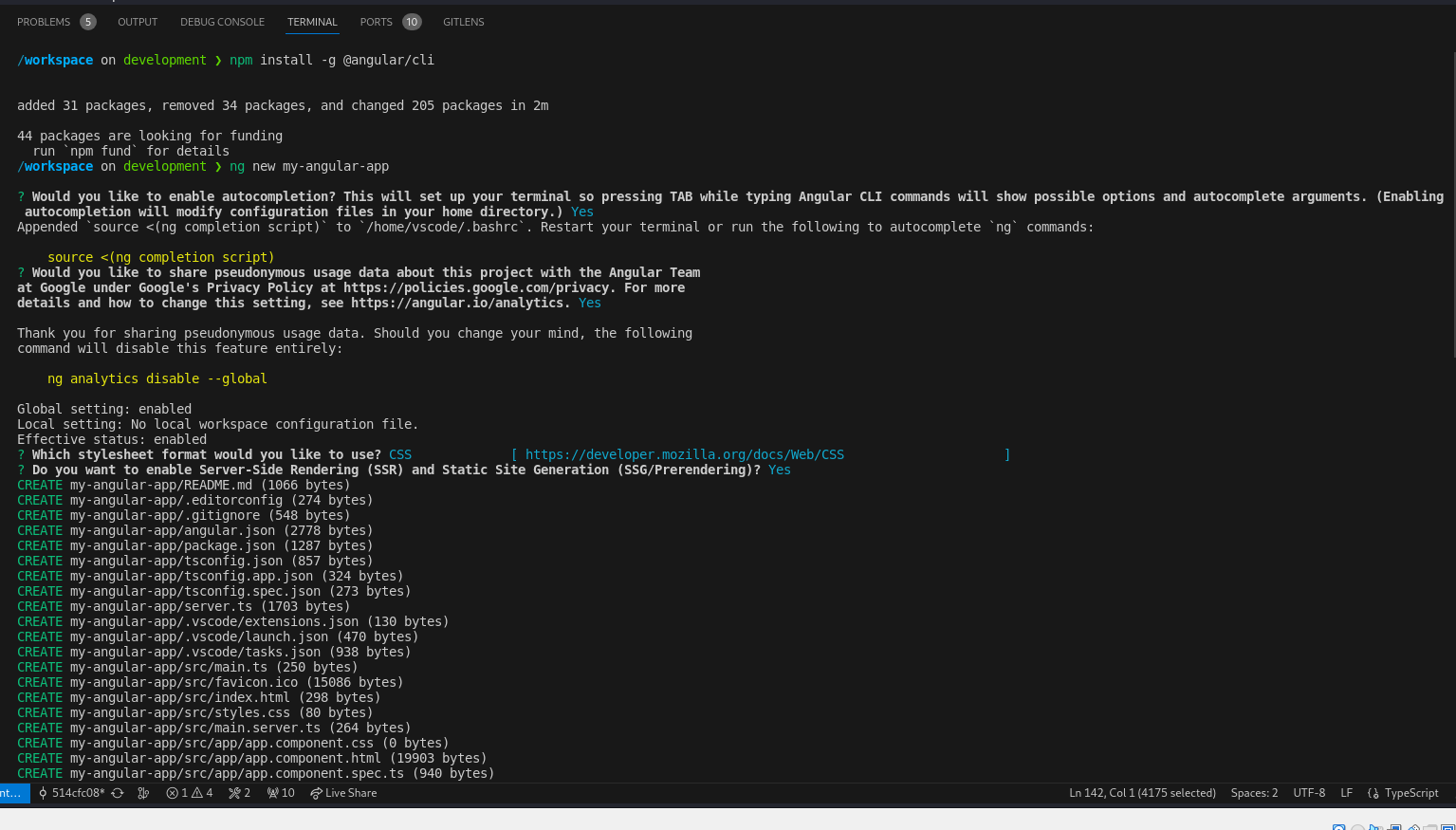
**Evidence**

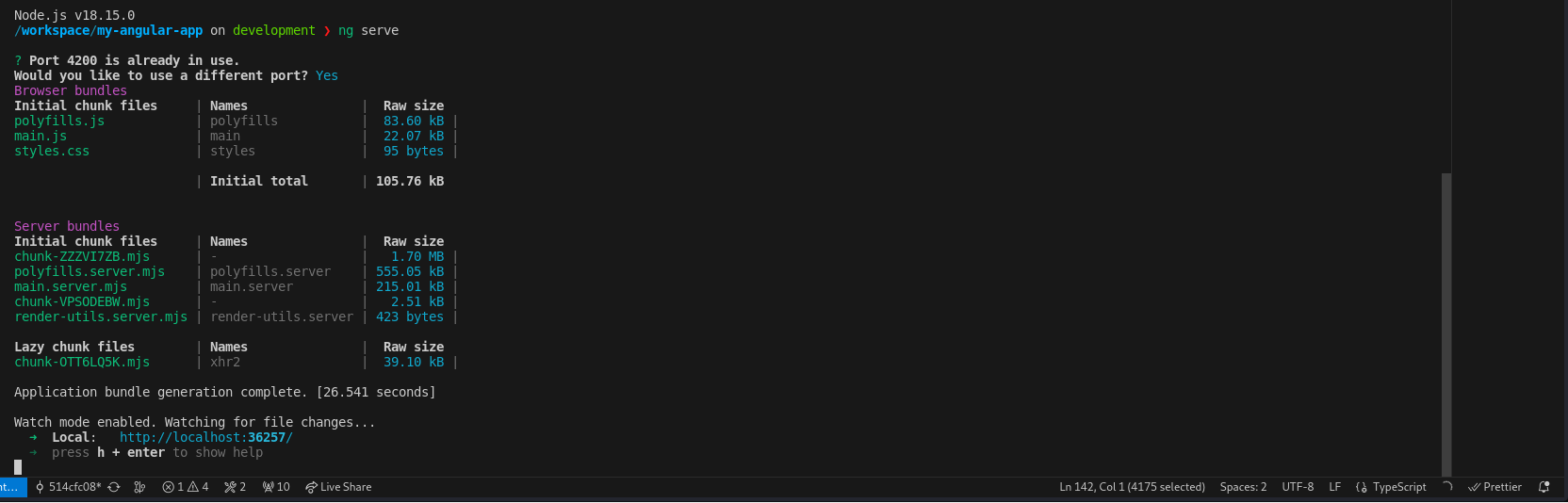
**Step 1:** I found that vulnerability in Path: /home/kali/doubtfire-deploy/doubtfire-web/b/src/app/sessions/states/sign-in/sign-in.component.ts through brakeman.



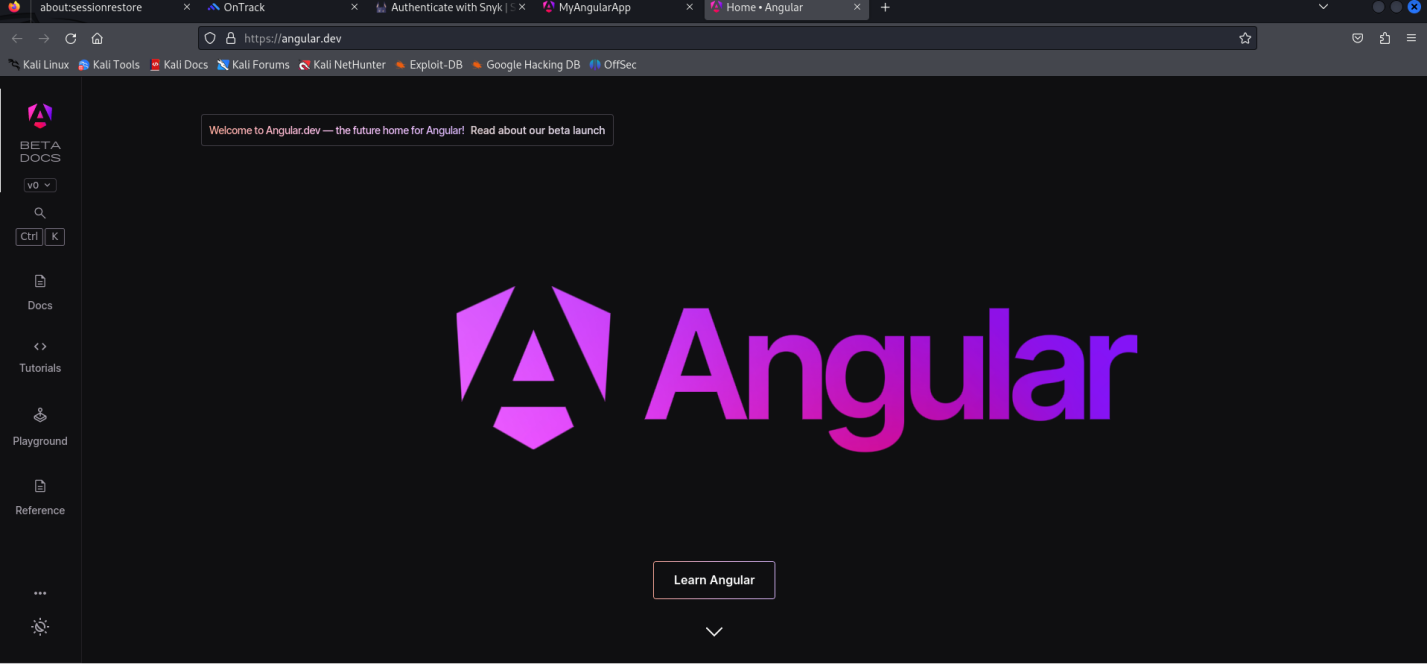
**Remediation Advice**

1. **Install Angular.js, open my-angular-app, Then open ng-serve**





1. This opens Angular.dev.



Remediating with Angular.js ensures robust security features, including data sanitization and protection against common web vulnerabilities. Leveraging Angular.js benefits from its active community support and framework-level protection, reducing the likelihood of security breaches. Additionally, Angular.js receives regular updates and patches, ensuring ongoing protection against emerging threats while maintaining scalability and ease of maintenance for the authentication process.

**References**

[AngularJS — Superheroic JavaScript MVW Framework](https://angularjs.org/)

**Contact Details**

Jaspriya Kaur

S222196102@deakin.edu.au

**Pen test Leader Feedback.**

The lead will provide feedback to enact on.