

**Finding Name:** Unencrypted Communications.

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

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

**Finding Description**

Sensitive information Disclosure in

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

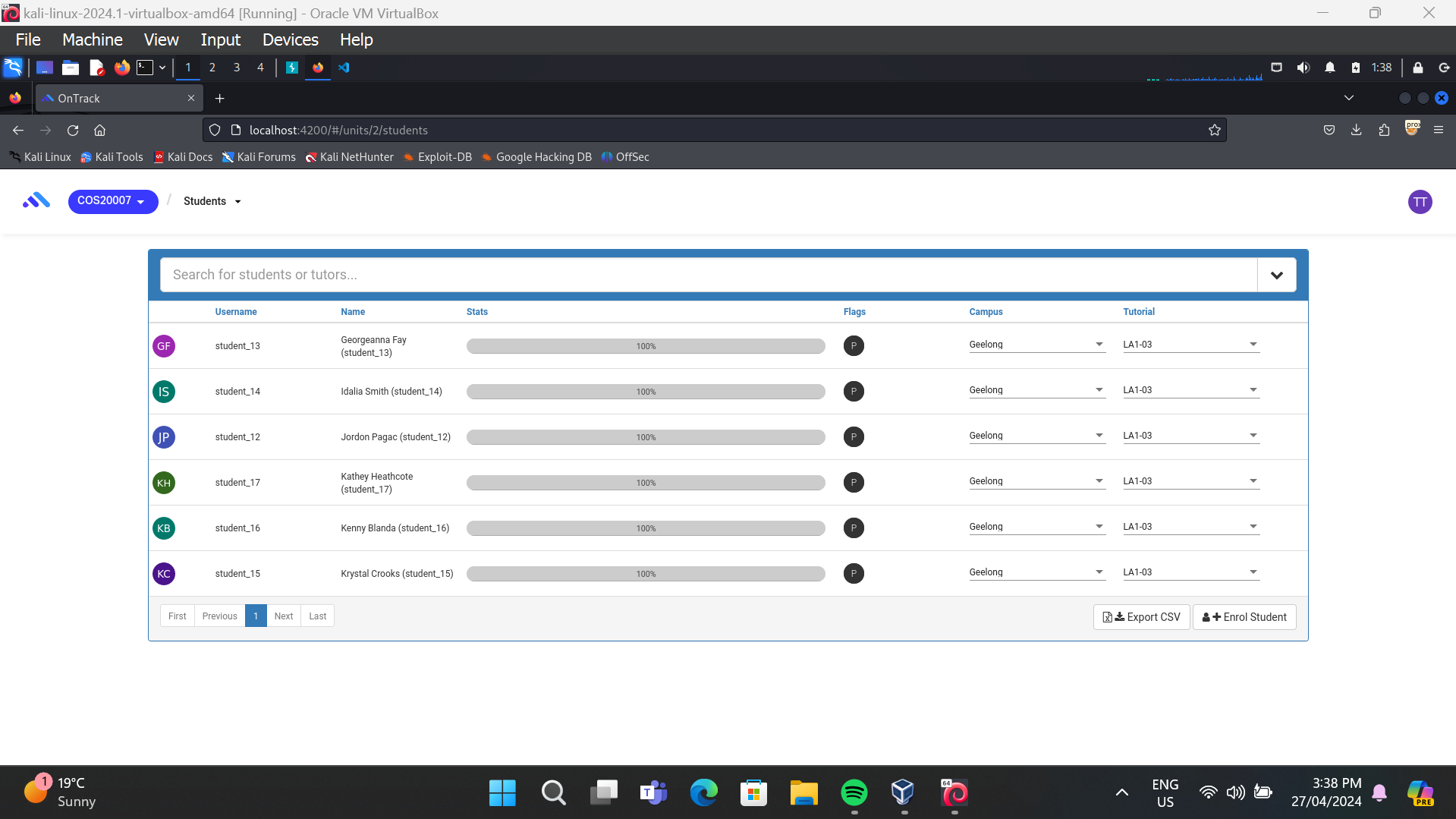
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant 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. |

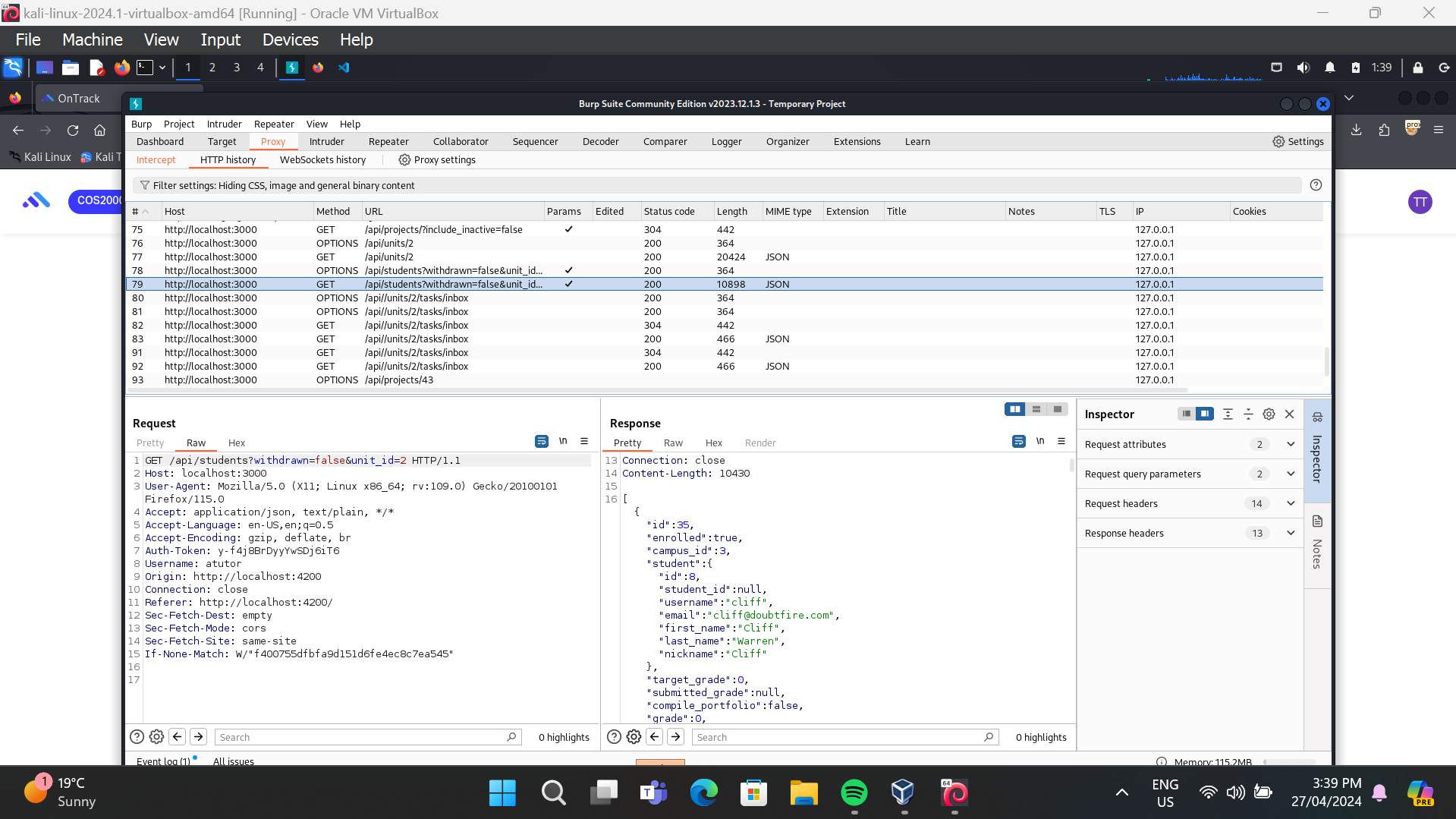
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur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

**Business Impact**

**Affected Assets**

**Evidence**

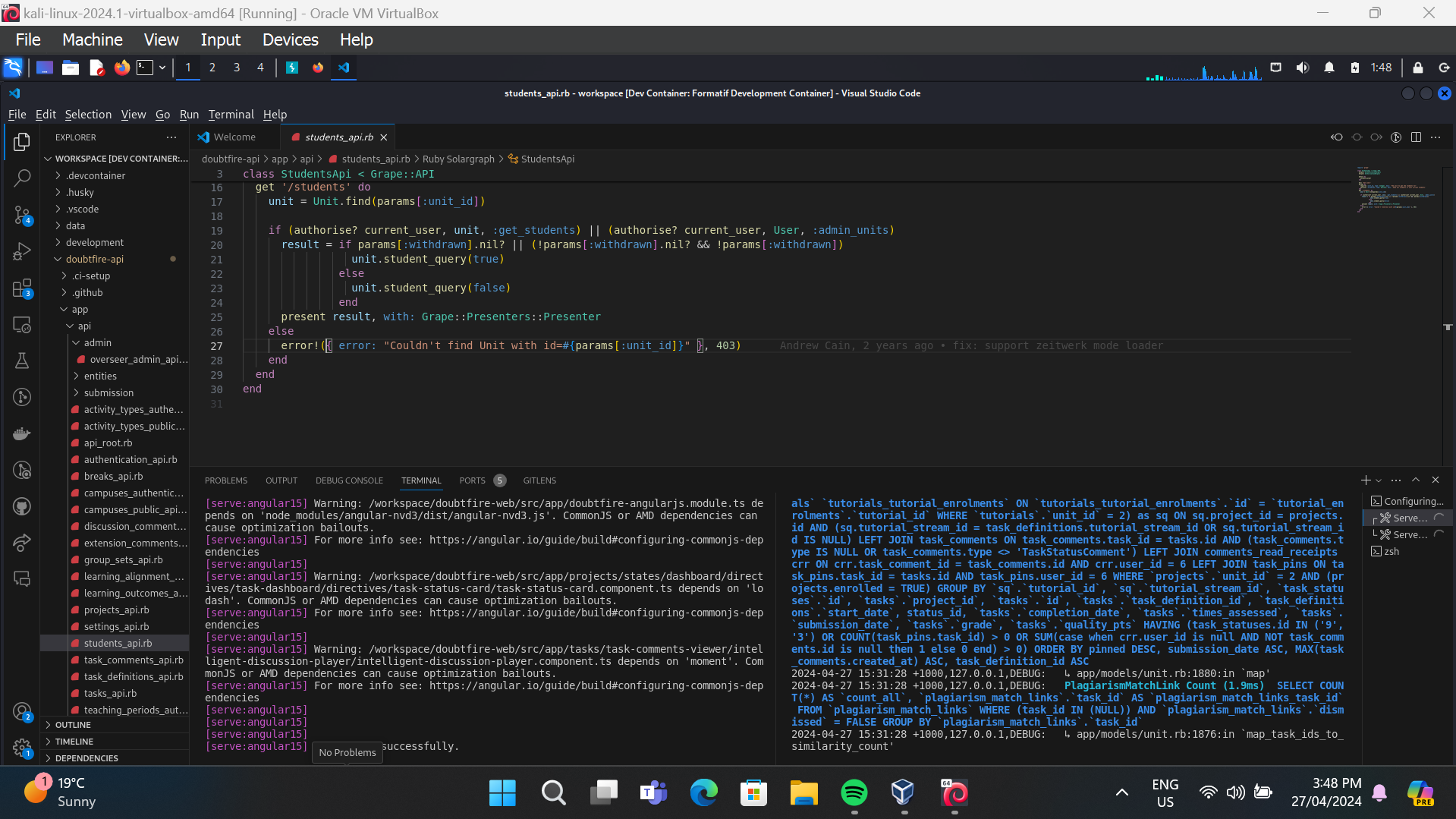
****

****

**Remediation Advice**

One possible recommendation should be:

**In the get '/students' endpoint, there is a condition checking if the user is authorized to access the student data:**

****

if (authorise? current\_user, unit, :get\_students) || (authorise? current\_user, User, :admin\_units)

This condition seems to allow access if either of the following conditions is met:

1. The current user is authorized to access the students of the specified unit (authorise? current\_user, unit, :get\_students).
2. The current user is authorized to administer all units (authorise? current\_user, User, :admin\_units).

If there's any flaw in the implementation of the authorise? method or in the authorization logic itself, it could potentially lead to an Authorization Bypass vulnerability.

For example, if there's a bug in the authorise? method that incorrectly allows access for certain users, an attacker could exploit this vulnerability to gain unauthorized access to student data without the proper permissions.

1. Review Authorization Logic:

Check authorise? method for accurate user permission validation.

1. Least Privilege Principle:

Grant minimal necessary permissions to users.

1. Parameterize Authorization:

Specify permissions based on roles, actions, and resources.

1. Input Validation:

Validate unit\_id and sanitize input parameters.

1. Test and Audit:

Thoroughly test and audit authorization logic for vulnerabilities.

1. Implement RBAC:

Use Role-Based Access Control for structured permission management.

1. Monitor and Update:

Regularly monitor for unauthorized access and keep security measures updated.

**References**

[**https://owasp.org/www-project-web-security-testing-guide/**](https://owasp.org/www-project-web-security-testing-guide/)

**Contact Details**

Name: Mohnish Sharma

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.