# API Security

## Background

The security of non-public APIs is crucial to prevent unauthorized data access. For instance, in our project, when modifications are made to the questions within a test, an attacker might change the question ID to one that was not created by them. This could lead to unauthorized modifications of other questions.

## Action items

- [x] Add an `owner` identifier in the database.
- [x] Before invoking the method, check if the `owner` of the data being modified matches the user information obtained from the current `JWT` token.

## Decisions

Implement RBAC and perform additional checks within API methods to verify user permissions for data access, thus preventing authentication bypass and cross-permission operations.

## Demonstration

Unauthorized modifications are not allowed.