

# 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

- ✓ Add an `owner` identifier in the database.
- ✓ 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.

POST

{{url}}/tests/save/

Params	Authorization	Headers (10)	Body	Pre-request Script	Tests	Settings
<input checked="" type="checkbox"/>	Content-type		application/json			
<input checked="" type="checkbox"/>	Content-Length		<calculated when request is sent>			
<input checked="" type="checkbox"/>	Host		<calculated when request is sent>			
<input checked="" type="checkbox"/>	User-Agent		PostmanRuntime/7.37.3			
<input checked="" type="checkbox"/>	Accept		*/*			
<input checked="" type="checkbox"/>	Accept-Encoding		gzip, deflate, br			
<input checked="" type="checkbox"/>	Connection		keep-alive			
<input checked="" type="checkbox"/>	Authorization		{{admin_token}}			
	Key		Value			Description

Body Cookies Headers (8) Test Results

200 OK 61 ms 368 B

Pretty Raw Preview Visualize

JSON

```
1 {
2   "statusCode": -1,
3   "message": "Failed to save test: Error: Test not found or unauthorised",
4   "data": null
5 }
```