

User Authentication and JWT

Background

To ensure data integrity and prevent tampering, our project employs user authentication using JWT.

Action items

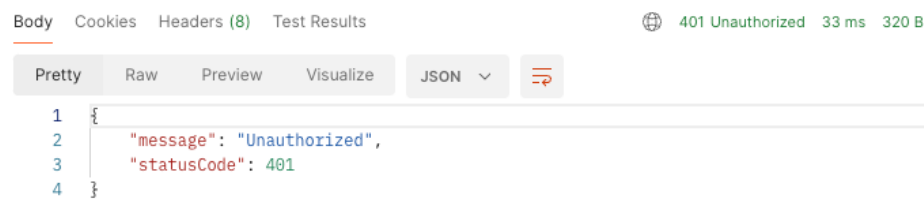
- ☒ Implement JWT token generator and verifier
- ☒ Implement User Roles for user authorization

Decisions

-  Implement JWT with a secret key to verify token signatures and set expiration times for tokens to prevent the use of old tokens.

Demonstration

Unauthorized operation will be captured.



The screenshot shows a REST client interface with tabs for Body, Cookies, Headers (8), and Test Results. The Body tab is selected, and the response is displayed in JSON format. The response is a 401 Unauthorized status with a message and status code. The response body is:

```
1 {  
2   "message": "Unauthorized",  
3   "statusCode": 401  
4 }
```