**Auth API Documentation**

**Base URL**: /api/auth

**Login**

* **Endpoint**: POST /api/auth/login
* **Description**: This endpoint allows users to log in using their username and password. If the credentials are valid, a JWT token is generated and returned, which can be used for accessing protected resources.

**Request Body:**

json

{

"username": "testuser",

"password": "password123"

}

**Response:**

* **200 OK**: Returns a JWT token if the credentials are valid.

**Response Example**:

json

{

"token": "your-jwt-token-here"

}

* **401 Unauthorized**: Returns an error message if the credentials are invalid.

**Response Example**:

json

{

"message": "Invalid credentials"

}

**Parameters:**

* **Body Parameters**:
  + username (String) - The username of the user.
  + password (String) - The password of the user.

**Errors:**

* **400 Bad Request**: If the request body is malformed or required data is missing.
* **401 Unauthorized**: If the provided credentials are invalid.