**General Steps to Implement Authentication and Authorization**

1. **Set Up Your Project**:
   * Start by creating a new Spring Boot project with dependencies for Spring Security, Spring Web, Spring Data JPA, PostgreSQL, and Lombok.
   * Configure your application.properties or application.yml to set up the database connection and other required properties.
2. **User Model and JPA Repository**:
   * Create a User entity class with fields like id, username, password, and roles.
   * Implement a UserRepository interface that extends JpaRepository.
3. **Password Encoding**:
   * Use Spring Security’s PasswordEncoder to hash passwords before saving them in the database.
4. **Security Configuration**:
   * Configure Spring Security to manage user authentication and define protected endpoints.
   * Implement a custom UserDetailsService to load user details from the database.
   * Set up JWT token generation and validation filters to secure your API.
5. **Controller and Endpoints**:
   * Create controllers for user registration and login. Upon successful login, generate and return a JWT token to the client.
   * Protect other endpoints with roles and JWT authentication.
6. **Testing**:
   * Test your application using tools like Postman or curl to ensure that the authentication and authorization mechanisms are working correctly.

Let me know if you need detailed guidance on any of these steps or any specific code examples!