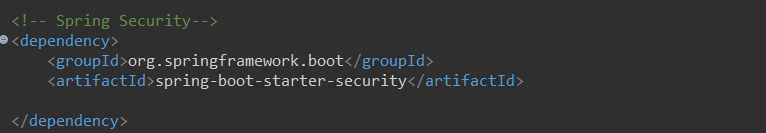
**Exercise 12: Online Bookstore – Securing RESTful Endpoints with Spring Security**

Business Scenario:

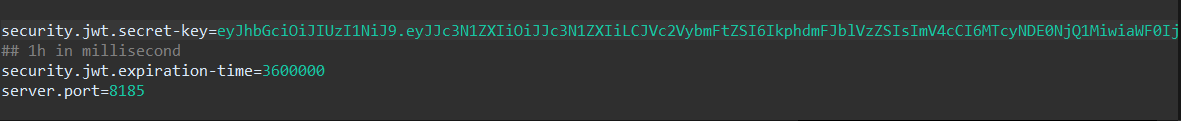
Secure your bookstore's RESTful endpoints using Spring Security with JWT-based authentication.

1. **Add Spring Security:**

* I integrated Spring Security into my project by adding spring security in pom.xml file:



Modified Application.properties:



I generated the JWT secret key using Online JWT Generator where I gave the Key as “parambrata\_5006856”:

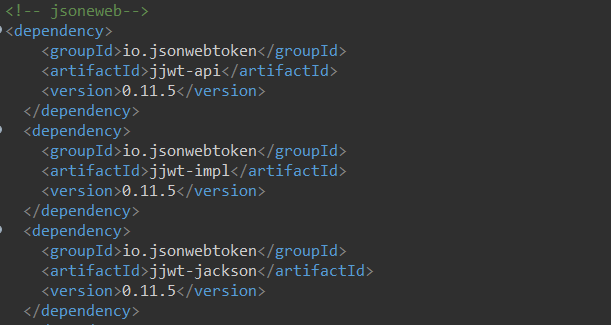


Clicking on Create JWT the secret key is generated.

1. **JWT Authentication:**

* I implemented JWT-based authentication and authorization:

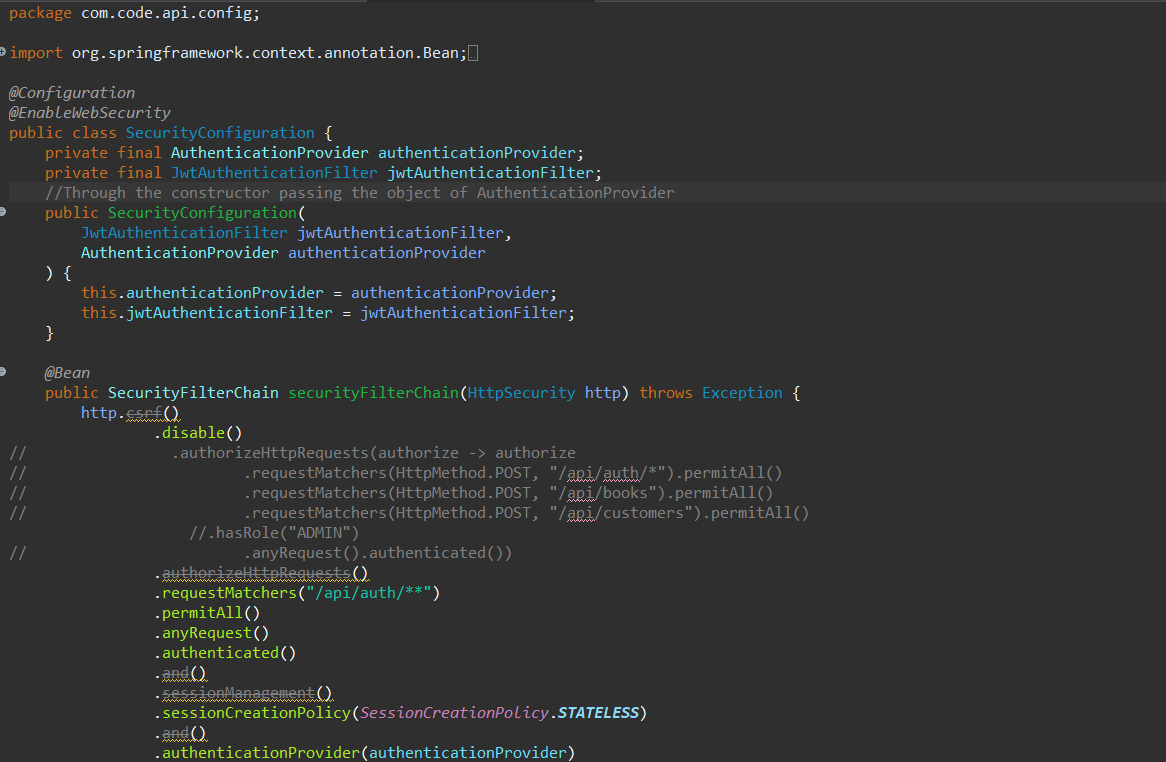
Added dependency for JWT support:

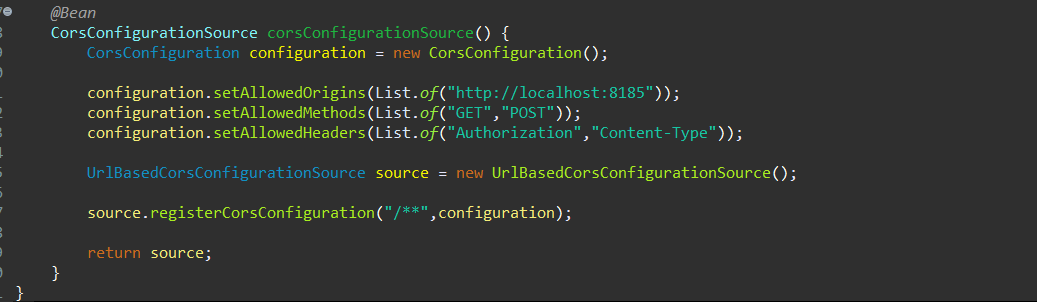


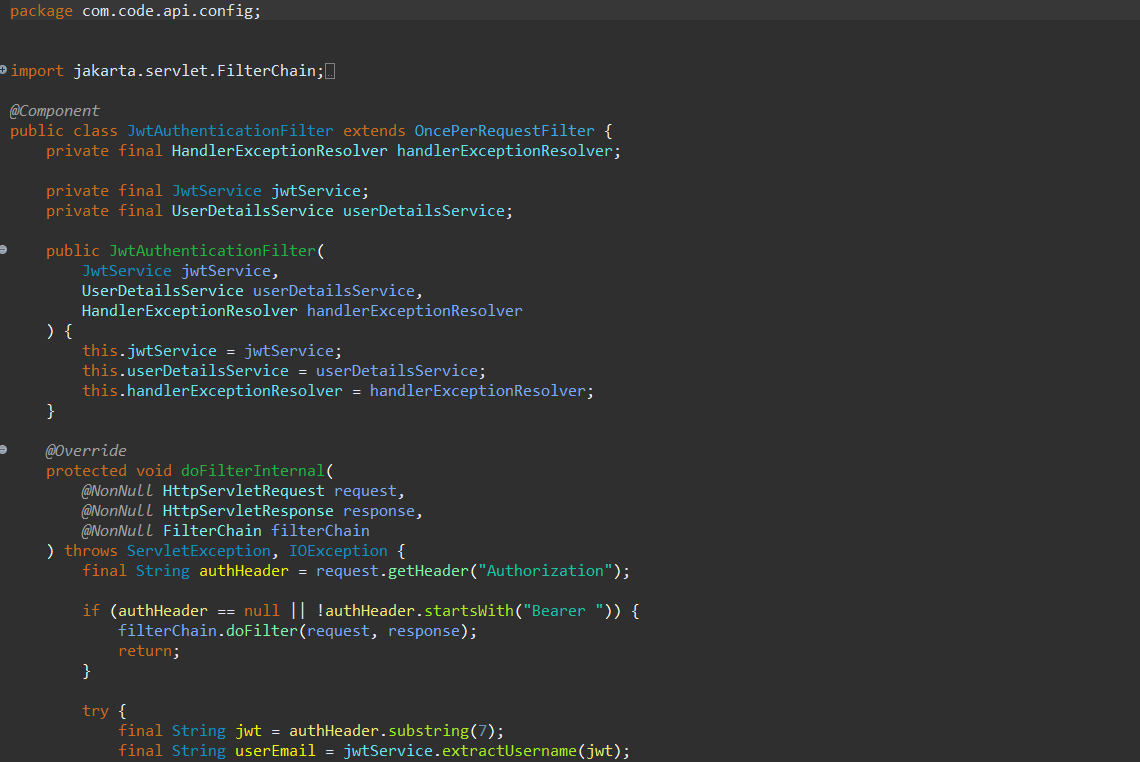
1. **CORS Handling:**

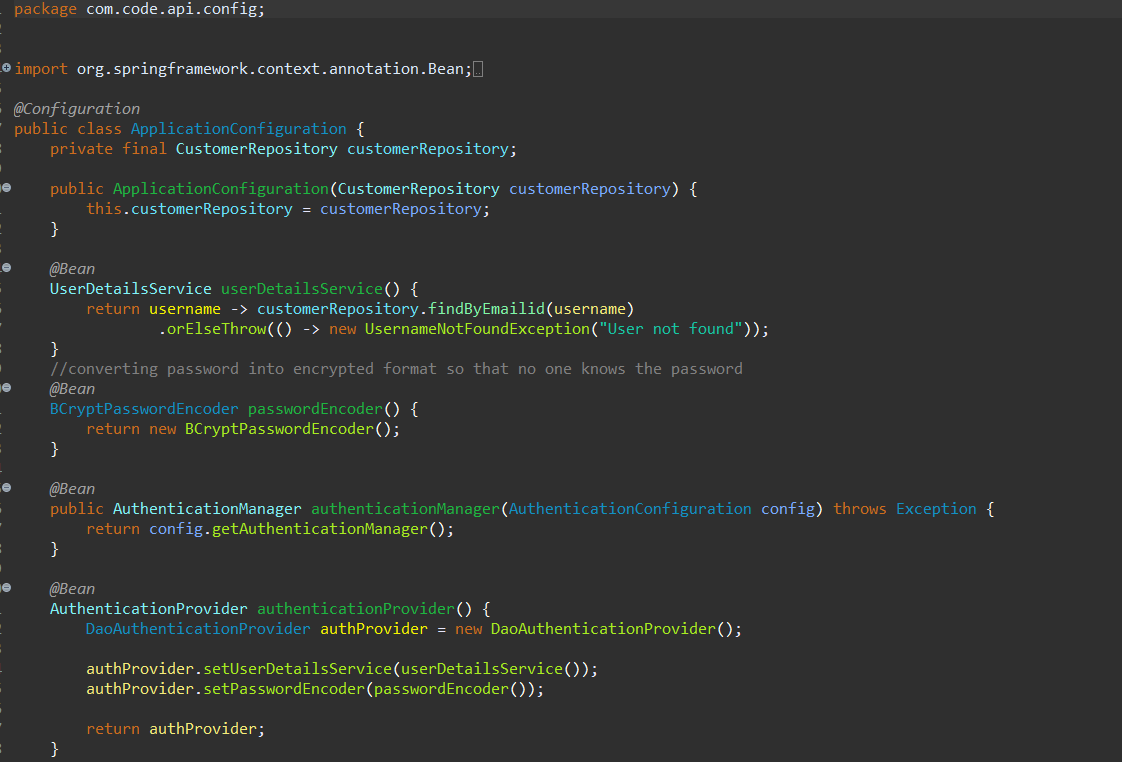
* I configured CORS to handle cross-origin requests:

The classes under “com.code.api.config” are as follows:

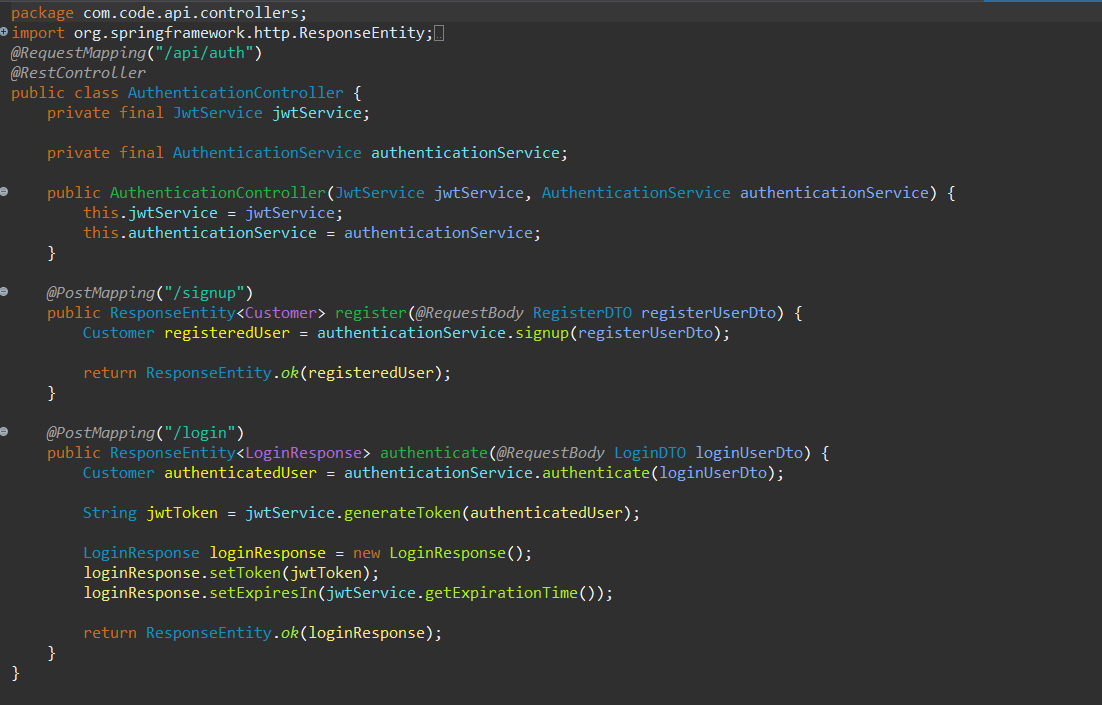


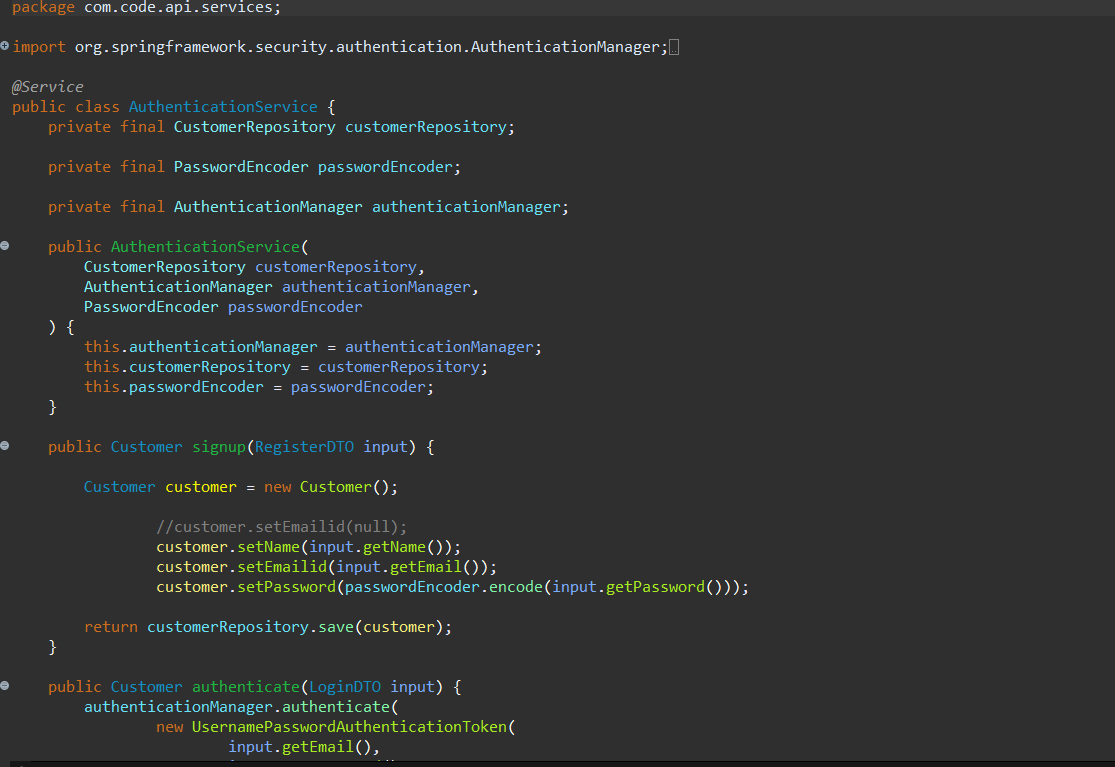




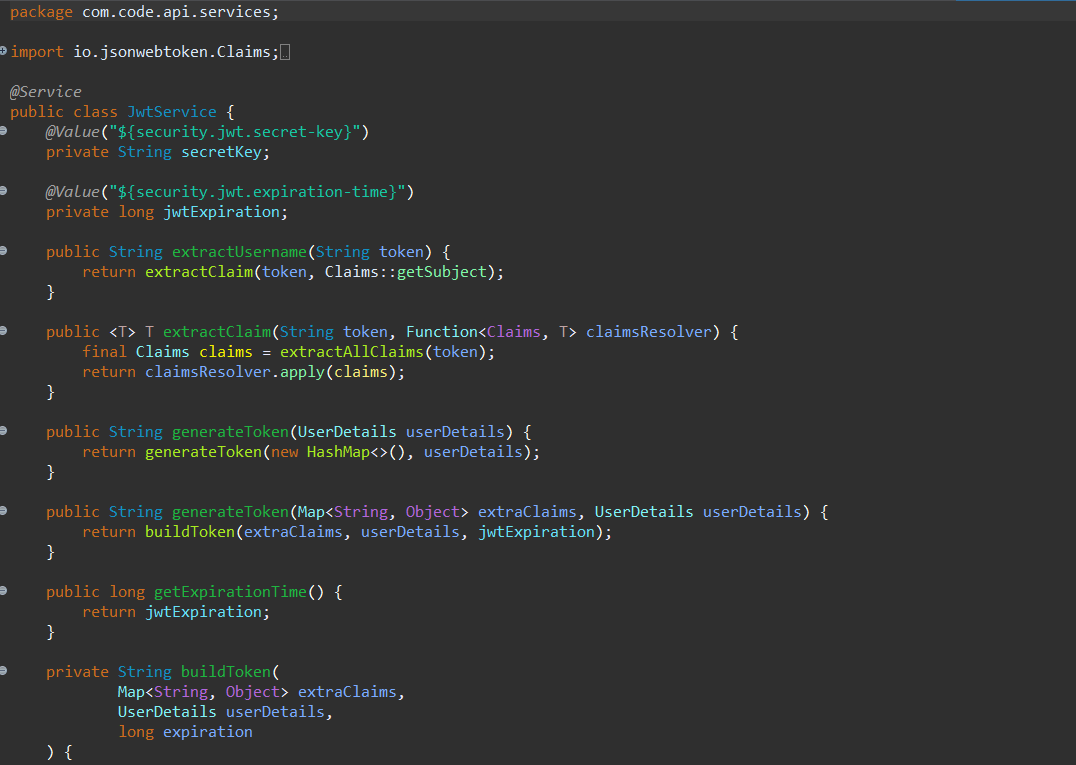


Authentication Controller and Authentication service:

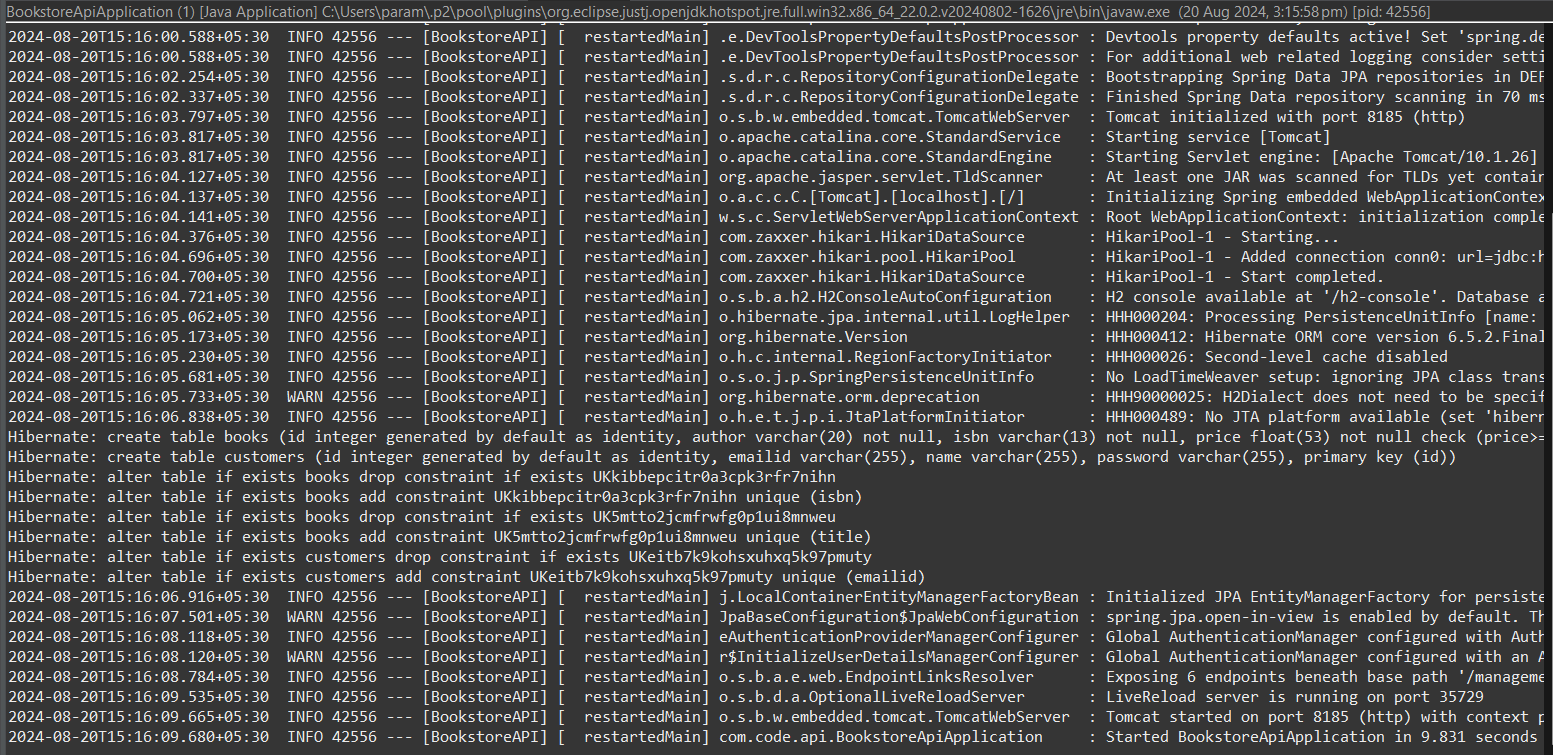




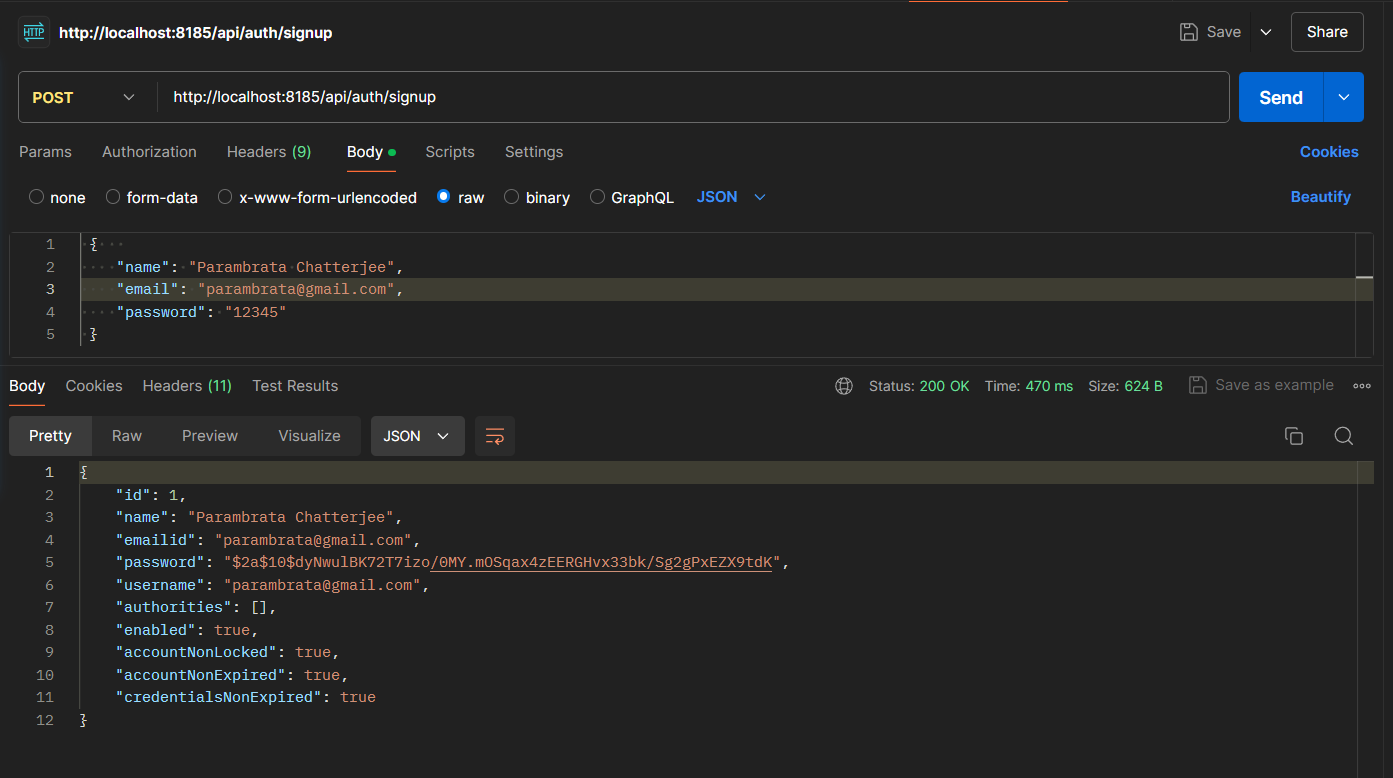
JWT Service:



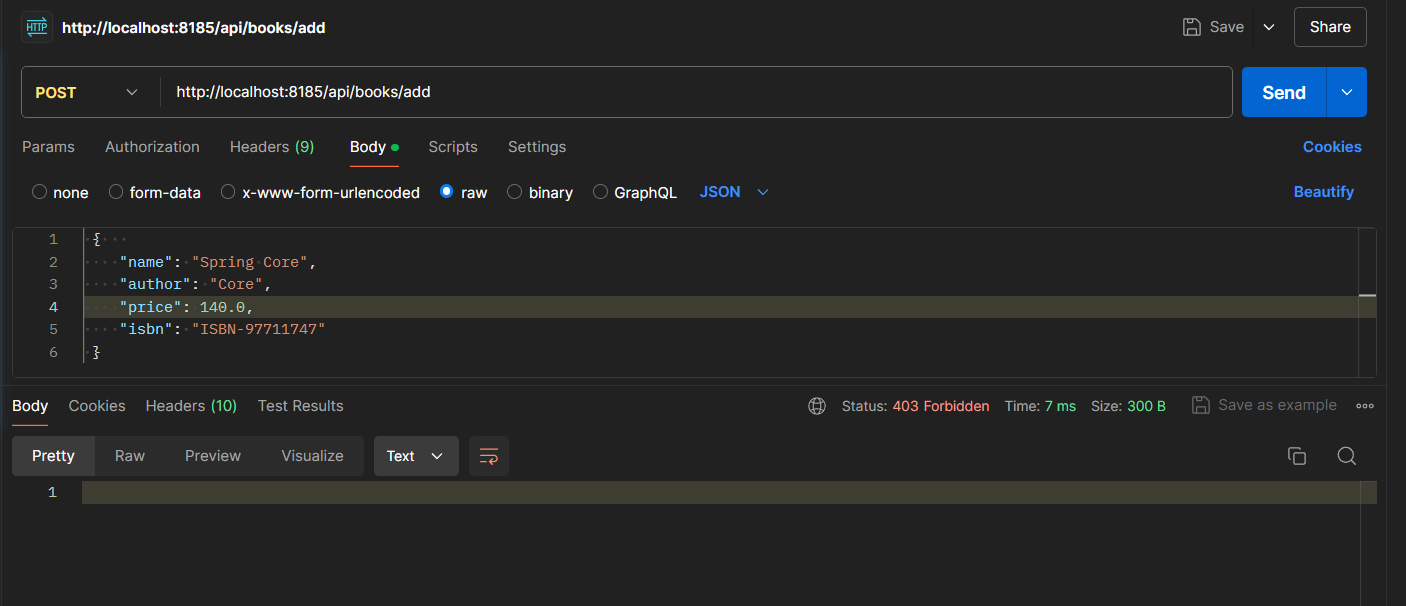
**Output:**



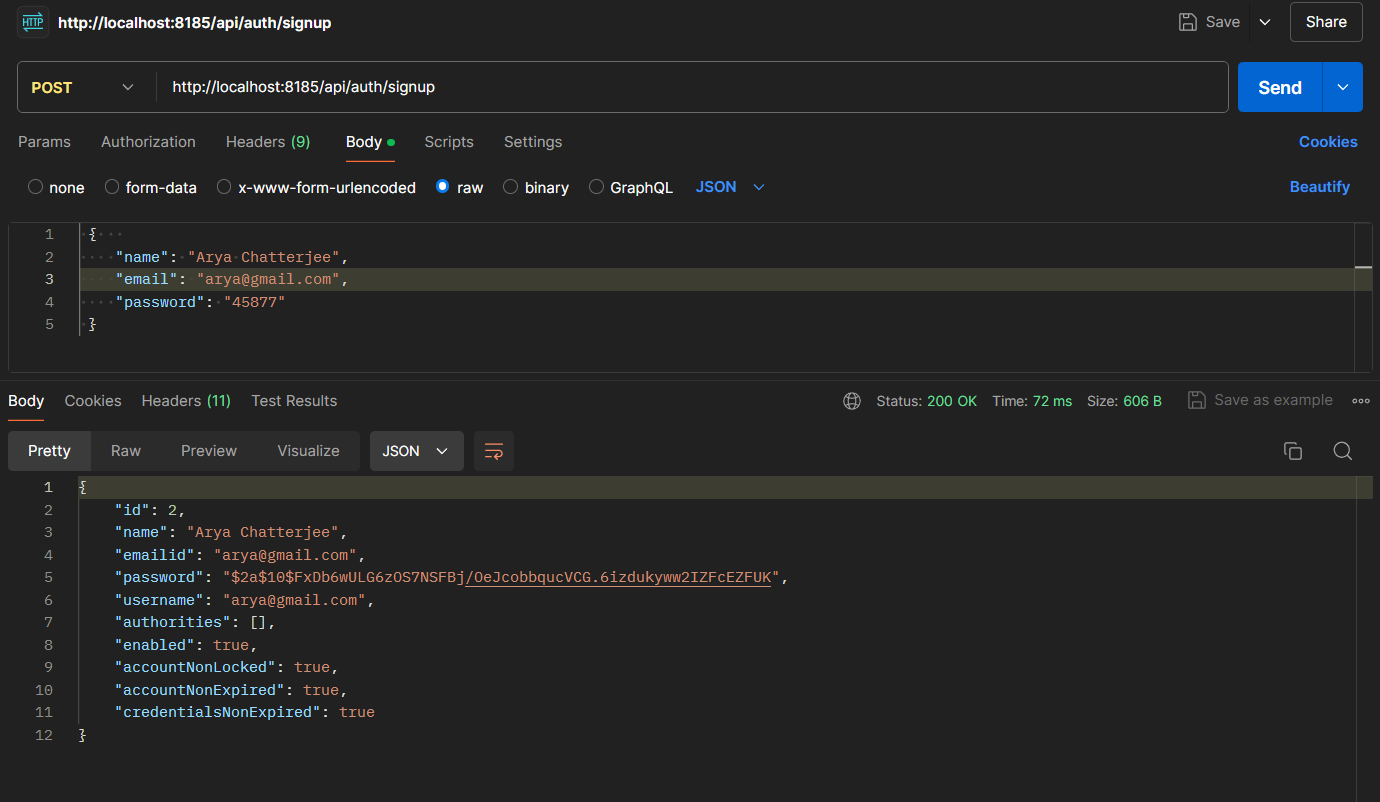
Sign-up:



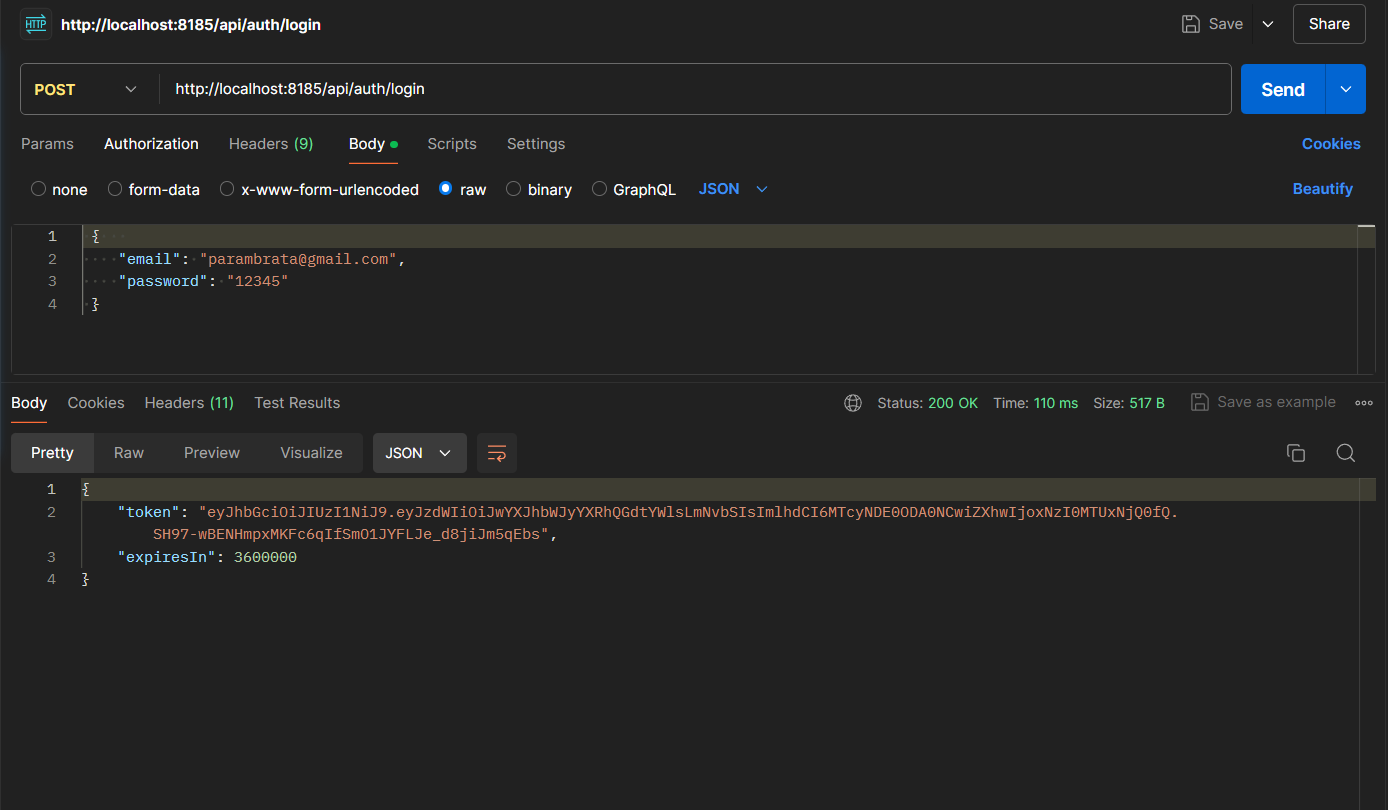
403 Forbidden:



Again signup:



Login:



Pasting the token and after 1 hour it will automatically expire:

