Day22 Spring Security – JWT (Auth Flow)

JWT – JSON Web Token (It’s a very popular Authentication & Authorization method)

Token based Auth.

JWT -Consist of 3 parts namely Header, Payload & Signature. – jwt.io

Token. (Secret key)

Spring Boot. – Spring Security

UserDetails. (username/email, password, authorities (roles) )

All endpoints are secured by default.

To access any endpoint, a valid session is needed.

/login, /logout – two end points will be automatically created.

Login Form & Logout form will be created automatically.

A default user with the username as “user” will be created and password also dynamically generated and displayed in console.

Instead of auto generating credentials we can add them in application.properties file.

(spring.security.user.name, spring.security.user.password, spring.security.user.roles)

Database based security. – (User credentials will be stored in database. Which will be retrieved during the login/registration time)- password will be saved in encrypted format.

JWT – JSON Web Token.

Server will create a session and Generate JWT and send it back to client.

JWT is time based. We can configure the expiry time of the token. 24\*60\*60\*1000 = 1 day

Authentication & Authorization

Airline Reservation System.

1. User Service (Registration[signup], Login[signin], update – profile update, audit columns, Forgot Password ) – ~~Captcha, Social Media based registration, Password expiry and reset after pre-set duration..~~
2. Reservation (Source, destination, journey\_date, no\_of\_passengers, name, age, gender, id, reservation\_number)
3. Ratings & Review (Enabled after completing a travel, Rating (1—5), comments/feedback, attachments [photos, videos, voice message etc.,]
4. Notification (SMS & Email) – After successful booking, cancellation of booking, [Java mail service]
5. Payments – We can integrate with 3rd party payments (stripe, PayTM, Gpay, etc.,)
6. Airlines (Name of airlines, operating cities, url)
7. Security (JWT/OAuth) [Register or Signup, Login or signin, Credentials Expired, User is Inactive, Duplicate Entry – User already registered] (Authenticate & Authorize – RBAC)
8. Airports (Add airport details, Unique Alphabet id(XXX), Name of the Airport, Address, Map Location(URL), etc.,)

<https://www.geeksforgeeks.org/springboot/spring-boot-3-0-jwt-authentication-with-spring-security-using-mysql-database/>

RBAC – Role Based Access Control – Based on the role of the user, different user will have different level of access to resources.

Day22rbac Springboot project

* Spring web, Lombok, data jpa, h2, mysql, postgres, mssql, security, devtools, actuator, JWT, Swagger

