Spring security

Add below dependency in pom.xml file

<dependency>

<groupId>org.springframework.boot</groupId>

<artifactId>spring-boot-starter-security</artifactId>

</dependency>

When we are adding this, by default spring will create a password.

So whenever you are accessing any API of your application , you will geet username, password screen.

Username= user and password = default password given in console

If you want custom username and password, then you can add following lines in configuration files

spring.security.user.name=sergey

spring.security.user.password=sergey

spring.security.user.roles=manager

Drawback: here this security is applied to all the API of an applications.If we have to secure any specific api, let see further.

**BASIC AUTHENTICATION USING IN-MEMORY DATABASE**

Here we are securing some APIs with some roles.

For this we need to take a class and annotate is with **@EnableWebSecurity** and extend the class by **WebSecurityConfigurereAdapter** class. It has several methods. Below we will see some methods:

One method is used to specify what are the APIs which are used by roles

One method is used to specify username, password, role

[Note: once you hit request and provide credentials, you will get your page. But if again you are hitting same url, now no authentication will be there]