Spring Security – To Secure your REST Api End points this module of Spring is used.

API – Application Programming Interface – Code RE-Usability

JDBC API – Helps to interact with any RDBMS using JAVA

JPA API- Java Persistence API – (Predefined Classes & Interface – ReUsing the built-in code to achieve the required functionality)

Employee

JDBC – Generic CRUD operation - Core JAVA project – Connect with any DB and do CRUD operation on any table.

Java FX , Angular, React

Generally API will help you to complete certain task

Web API/REST API/SOAP API – We are going to get some services with the help of internet by calling some end points. –XML/JSON output.

JDK – String, StringBuilder, StringBuffer, Thread

Java.lang – no need to import (String, wrapper classes)

List, Map, -- java.util

Java.sql or javax.sql

Javax.persistence

Spring Security – It’s a module in Spring Framework. Using that we secure our endpoints.

Adding the spring security dependency to the spring boot project will

1. Create two end points namely “/login” & “/logout”
2. Create a GUI page with the login form to authenticate the user
3. Also creates a default user and generate random password which will be displayed in the console.
4. After successful login validation, spring security allows us to access any end point
5. In case of wrong credentials, we will get a error message “Bad Credentials” in login page.

Configuring Spring Security

1. Using application.properties file (Add Few properties)
2. Using Java Code (Hard coding the user details)
3. Using spring data jpa and reading the credentials from DB

Password Encoder – Convert normal password to encrypted password

1)NoOpsPasswordEncoder

2) BCryptPasswordEncoder

ThymeLeaf – GUI for Spring Boot App (html+ Java code with spring boot)

<https://www.kindsonthegenius.com/introduction-to-spring-security-a-practical-tutorial/>