As we created the Application till now but we it’s not secure so I’ll add spring security so it will work like shield for application , it means it will secure the application and then we can customize the security on our need basis server

Why Spring Security

App server

spring security

User

who you are, what you want

# It is application security framework

->Login and Logout functionality

->Allow/block access to URLs to logged in users

-> Allow/block access to URLs to logged in users and with certain roles

->flexible and customizable

-> handle vulnerabilities

->widely adopted so we can get lot of resources and support from internet and quick response

## What Spring Security can do

->User name/password authentication

->App level authorization

-> intra app authorization like oAuth

->Microservice security(Using tokens,JWT)

->Method level security

5 core concepts in spring security

### Authentication, Authorization, Principal, Granted Authority, Roles

now let’s understand each points one by one

App server

spring security

User

who you are, what you want

Here when spring security asks you question WHO YOU ARE and you provide the identity who you are then it’s authentication

when you go to any site like facebook and asks you this question and you provide username and password or any other information and you gives then it’s called knowledge based authentication

## Knowledge based authentication

->password

->Pin Code

->Answer to a secret/personal question

->easy to implement and use

However it’s comes with disadvantages also

suppose someone steal your password or find you password then they can login using your account that’s the problem

other type of authentication like

possession based authentication

->Phone/text messages

->key cards and badges

->Access Token devices

## Multifactor authentication

it is combination of knowledge based+possession based authentication

->enter your password then verify your text messages

#### Authorization

### Can this user do what they trying to do-> Yes/No

->For authorization user first should be authenticated

#### Principal

->it means currently logged in user or account

->one user can have multiple accounts so principal will reflect to currently logged in account

#### How authorization happens

Here is a concepts comes granted authority so we can configure the authority for like manager, user, management department what they can do and spring security will take cares of the rest

## Roles

->Group of authorities

suppose if we have manager and management department have same access so instead of writing same permission for both we can give the role and assign the permission we can set the role Like ADMIN and USER

->Spring security will do all this automatically by adding the dependency of spring security

now we will add spring security dependency

<dependency>

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

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

</dependency>

Now automatically our application got secured now when we will access any url let’s say /users the it will automatically redirects us to the login page and opens the login form and default username will be user and password will be auto-generated and now we can customize our application security on our need basis

Now understand how spring security do all this

->the answer is something called Filters , it is basis servlet technology

A filter is an object used to intercept the HTTP requests and responses of your application. By using filter, we can perform two operations at two instances −

* Before sending the request to the controller
* Before sending a response to the client.

Server

Filter

Filter will authenticated the user, if it is verified then request will go forward otherwise request will be returned

#### Spring Security default behaviour

->Adds mandatory authentication for all the URLs

-> Adds login form

->Handles login error

->creates a user and set a default password

->by default username is user and password is auto-generated , spring security generates a new password each time you start the app

now if want use our custom username and password for example username scooby and password 123 then we go inside application.properties file and mention

spring.seurity.user.name=Scooby

spring.security.user.password=123

#### How to configure authentication in Spring Security

when we add spring security dependency then it creates default user and put your application behind form based authentication, we can obviously configure what will be the default user in the application.properties file but it’s not ideal because we want to have spring security authentication based on the multiple users present in the database or in some external states

now the way to configure authentication in spring security is by affecting what’s called the AuthenticationManager