**Spring Boot Actuator – Security**

**Spring Boot Actuator – Security**:

We can expose all the different Spring Boot actuator endpoints. But this is not secure. Anyone can access this sensitive data. We may NOT want to expose all of this information to anyone on the web. So, we have to secure the data. For this we have to add Spring Security to project and endpoints are secured.

**Add Security**:

For add security add the following dependency to our "**pom.xml**" file.

<!-- Add security to our project -->

<dependency>

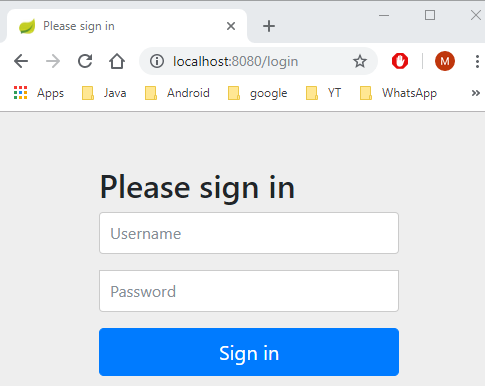
<groupId>org.springframework.boot</groupId>

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

</dependency>

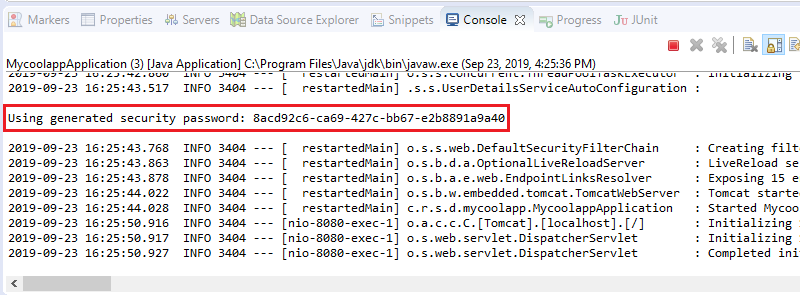
**Secured Endpoints**:

* Now when we access: **/actuator/beans**
* Spring Security will prompt for login



Here the default username is **user** and password by default generate by the Spring container and displayed in the console.

"Using generated security password: fd7d3446-78d8-43c1-ac9a-6a8abbf9d80f"



**Spring Security configuration**:

We can override default username and generated password

**File: src/main/resources/application.properties**:

spring.security.user.name = ruhul

spring.security.user.password = odduu

**Excluding Endpoints**:

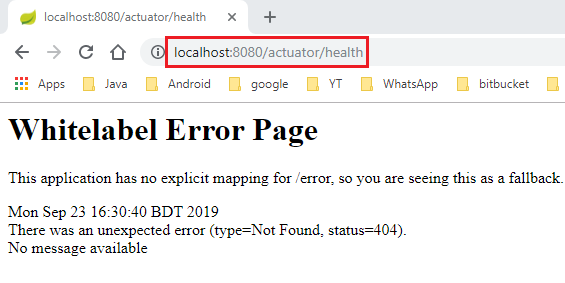
To exclude "**/health**" and "**/info**"

**File: src/main/resources/application.properties**:

# Exclude individual endpoints with a comma-delimited list

# management.endpoints.web.exposure.exclude=health,info

management.endpoints.web.exposure.exclude=health, info



**For more info**:

<https://docs.spring.io/spring-boot/docs/current/reference/htmlsingle/#production-ready>

**Development Process (Step-by-Step)**:

1. Edit pom.xml and add spring-boot-starter-security
2. Verify security on actuator endpoints for: /beans etc.
3. Disable endpoints for /health and /info

Spring Boot Actuator - Security