



Spring Security -using DB

In Previous exercises, you understood how to configure security credentials in memory. In this exercise, you will understand how to configure security credentials in DB

In this lab, u will be working on 03spring-security-db-start project

1) Open /WEB-INF/security.xml . Complete TODO -1 by configuring Jdbc Userservice as below ;

```
<security:jdbc-user-service data-source-ref="ds"/>
```

2) You need to make sure that default tables users and authorities are created. Open scripts.sql given to you under src/main/resources. and create users and authorities tables in db using the queries. Insert some data by executing the insert queries given to you.

3) Deploy the application and try to login with credentials configured in db.

Scenario-2

1) We dont want to use default tables. We want to use our custom tables. In such case, we can configure our own queries as below :

```
<security:jdbc-user-service id="jdbcuserservice" data-source-ref="ds"  
  users-by-username-query="select username,password,enabled from users where username=?"  
  authorities-by-username-query="select username,authority from authorities where  
username=?" />
```

2) Deploy the application and check that it works like earlier.



Scenario-3

1) **We want to group roles and assign users to groups**

2) **Open scripts.sql and create tables groups,group_members and group_authorities .
Populate those tables using the insert queries given.**

3) **Now Configure jdbc-user-service as below**

```
<security:jdbc-user-service id="jdbcuserservice" data-source-ref="ds"
group-authorities-by-username-query="select g.id, g.group_name, ga.authority from
groups g, group_members gm, group_authorities ga where
gm.username = ? and g.id = ga.group_id and g.id =
gm.group_id"/>
```

3) **Deploy the application and check if it is working as expected or not**

4) **can u think what we have to do if we want to use group names in intercept urls instead of role names?**

**Congratulations !! U have understood how to configure
Security credentials in Database.**