COS30041 Creating Secure and Scalable Software [Java EE]

62 Credit Task 7.2 Security – JDBC-realm

Time Frame: Weeks 8 – 10
Suggested to start in Week 8 and complete in Week 10
Submission Due: Week 11, Fri, 6:30pm

Overview

This task is about extending the "Secure-EMS" enterprise application in Pass Task 7.1 so that the application can access role-based authentication and authorization credentials (e.g. user id/user name/user email and password) stored in a separate database table and the password is stored in as encrypted format. **Since we have not discussed how to do this in lectures, it is left to you to devise and enact your own plan to independently research and learn about the technologies.**

Note: After completing this JDBC-realm, any new user added to the "Secure-EMS" database table(s) can access the relevant CRUD operations in the system. Remember you need to test this as well.

Purpose	To develop an enterprise application in which users' credentials and role based authentication information are stored on a separate database table
Tasks	1. Research into how to perform authentication and authorization 2. Develop an enterprise application and configure the enterprise server so that the application could utilize users' credentials and role based authentication information stored on a separate database table 3. Prepare your test cases and test your application thoroughly by using appropriate input values and database contents
Pre-req Task[1]	Pass Task 7.1
Follow-up Task[2]	
Suggested Time	4 hours if you know the stuff well 8 – 10 hours if you need to read the concepts and know how to establish database connections on the GlassFish server
Resources	Lecture 07a Security Java EE Tutorial – JDBC-realm
Feedback	Ask your tutor for feedback
Next task	

Credit Task 7.2 Submission Details and Assessment Criteria

You must create your own document (pdf) in **portrait** mode[3], which you will upload to Doubtfire, with the following details:

- Your name and student id
- Your tutor's name
- Your own responses to the tasks according to the corresponding instructions (see below)

[1]You need to complete the pre-requisite task before doing this task.
[2]You need to complete this task in order to do the follow-up task because the follow-up task depends on your answer in this one.
[3]Landscape mode pdf does not work properly in Doubtfire.

Background

Assumption: **You have completed Pass Task 7.1**

Tasks and Instructions

Task 1. Independent research and study

a. Research into how an enterprise application can authenticate and authorize users based on their roles stored in a database table.
b. In case you have multiple options for Task 1a, determine and explain which one you are going to use (e.g. easier, more reliable, less programming work, …). Justify your answers. e.g. one option is to use email address and password.

Task 2. Programming and Configuration Task [Assume you have completed Pass Task 7.1]

Enhance your enterprise application in Pass Task 7.1 so that your GlassFish server can now access login credentials and users' role stored in a separate database table (e.g. EMS_EMPLOYEE or another database table in your design to address the security concerns in Secure-EMS app in Pass Task 7.1). The requirements are as follows:

- Choose one option: e.g. use email address and password to access EMS
- The password should be stored in the table as encrypted format.

Hints: if you use jdbcRealm, you should choose "SHA-256" for "Password Encryption Algorithm". You should "hash" the password using SHA-256 algorithm, so the size of password field in the database table would be different from previous one.

Task 3. Testing

Write your test cases (including the database content and input values) and test your work thoroughly. Remember to collect your screen dump to show the evidences.

Submission Task

Once completed, you need to submit a pdf file that contains all your work (e.g. selected code segments – show the key stuff and some screen dumps of your testing)

Demonstration

You may be asked to demonstrate your assignment in the lab. You should be able to do this and explain your code when asked in the lab session.