COS30041 Creating Secure and Scalable Software [Java EE]

07 Pass Task 7.1 Securing your Enterprise Application

Time Frame: Weeks 7 – 10
Suggested to start in Week 7 and complete in Week 10
Submission Due: Week 10 Fri 6:30pm

Overview
This task is about a case study on the security concerns of an enterprise application. You are given a scenario of a "secure" enterprise application, you are required to analyze the situation, discuss any potential security concerns in terms of the "AACD" security principles (that is, Authentication, Authorization, Confidentiality and Data Integrity), and suggest any improvements and, finally, design and implement the application based on your suggestions. Remember, the focus of this task is not about protection from hacking.

Purpose	• To design and describe an architecture of an enterprise application, and relate these to any security issues and concerns of the application, and how to mitigate the potential threats • To develop an enterprise application based on the given business scenario so as to mitigate any potential threat raised by security issues and concerns, and related these to the choice of enterprise technologies used in the application
Tasks	1. Register security roles in GlassFish server 2. Secure an enterprise application 3. Read the Case Study 4. Analyze the security concerns of an enterprise application 5. Design an architecture to secure the enterprise application, and relate the architecture to those security issues and concerns 6. Develop the enterprise application based on your suggestions in Task 5 above 7. Prepare your test cases and test your application thoroughly by using appropriate input values and database contents
Pre-req Task[1]	
Follow-up Task[2]	
Suggested Time	4 hours if you know the stuff well 10 – 20 hours if you need to read the concepts and know how to establish database connections
Resources	Lecture 07 Security
Feedback	Ask your tutor for feedback
Next task	9.9P LSR feedback

07 Pass Task 7.1 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.

Tasks and Instructions

Task 1. Complete Lab_07a_Secure_GlassFish

Task 2. Complete Lab_07b_Secure_EMS

Task 3. Read the following Case Study section before proceeding

Case Study – A Secure Company's web-based Employee Management System (Secure EMS)

Background

SECURE is a company proud of developing secure enterprise applications. The company has a "secure" web-based system, called Employee Management System (EMS) to manage (that is the CRUD operations) its employees' records. Only the administrators of the EMS can login to the system and perform the normal CRUD operations. The current login credentials of the Administrators of EMS are stored in the GlassFish server as the "ED-APP-ADMIN" group (See Lab_07a_Secure_GlassFish for the credentials). Administrator can add, delete, edit, and review individual employee's record. All information of an employee's record (except the employee id, the primary key) can be changed including individual employee's password.

In Lab_07b_Secure_EMS, we make the application secure so that only users with "ED-APP-ADMIN" credentials can perform the CRUD operations of EMS.

Current Situation

The company is going to extend EMS so that its employees can manage their own data. It has at least the following requirements:

1. There are two different group of users in the system, namely Administrator and Employee.
   a. Administrator should login using the user's credential in the group of "ED-APP-ADMIN" (See Lab_07a_Secure_GlassFish for setting the credentials on GlassFish server)
   b. Employee should login using the user's credentials in the group "ED-APP-USERS"
   c. These credentials are stored onto the GlassFish server (after Lab_07a)

   Note: The user credentials used in this Pass Task is different from the one stored in the EMS's database. In the Credit Task, you will be given a chance to rectify this problem via using the security realm called JDBC-realm. After doing that, users will be able to login to EMS using their passwords stored in the EMS's database.
2. Administrator can add, delete, edit, and review individual employee's record as usual. All information can be changed including individual employee's password.
3. Employee can review their own details (excluding password), but not other employees. The decision of not having the password being viewed by individual employee (actually the password being sent to the web browser) is to protect them.
4. Employees can change their own details (including password), but not other employees.

For the following tasks (Tasks 4 – 7 below), you only need to focus on the Web-based Application of Secure EMS, no need to do the AppClient project.

Task 4. Analysis Task

4.1. In the context of the employee's CRUD operations on their own record, why the system does not allow employee to perform the "C" and "D" operations? Justify your answers.

4.2. In the context of the employee's Review operation, what information can be reviewed? Justify your answer.

4.3. In the context of employee's Review operation (reviewing their own detail), the company decided to implement a DTO which excludes the password being sent to the client. Why password is excluded? Do you think that this is a good practice? Why or Why not? If not, propose an alternative and justify your choice.

4.4. In the context of the employee's Update operation,

4.4.1. What information can be updated? Are these the same as those in 4.2 and 4.3 above? Why or Why not? Justify your answer.

4.4.2. What information cannot be updated? How would you avoid these data being updated by the employee "accidentally"?

4.5. In the context of the employee's Update operation, where should the actual change of the employee's information occur? Do you think this is a good practice? Why or Why not? Justify your answer.

4.6. In the context of employee's Update operation, the company decided to first display the details of a particular employee (if such employee exists after searching through the database via the employee's id) in the web browser so that the employee could enter the required information. Should the existing password be

(1) sent and displayed to the client?
(2) sent to the client but not displayed?
(3) not sent?

What is your choice? Why or why not? Justify your answer. If your answer is (3), how would you implement the feature that allows the employee to change their own password?

4.7. In the context of deleting employee's record, the company choose to accept the employee id as the input and then remove the employee record by setting the field "active" to false instead of removing the record from the database. Do you think that this is a good practice? Why or Why not? If not, propose an alternative and justify your choice.

4.8. After reviewing the features provided by the application "ED-Secure", do you think that the application as is can provide the features listed in the Case Study Section above? Are there any deficiencies? Why and why not? What changes would you suggest to address all features listed?

Task 5. Design Task [Assume you have completed Task 4 above]

Based on your comments / answers in Task 4 above, design the application to make it "secure" in terms of the "AACD" security principles (that is, Authentication, Authorization, Confidentiality and Data Integrity). You need to

a. Extend the given architecture diagram of the system to include your software components. Remember to show the interactions of the various software components. Your diagram needs to name each individual business and entity objects / classes, put them in the right Tiers (e.g. Business Tier including BLL and DAL, or Data Tier).

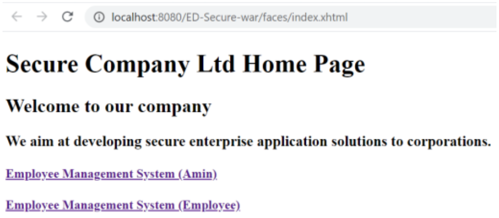
b. Describe and discuss the role of each component in your diagram.

In your discussion, you need to justify how you mitigate the potential threats raised by each of the security issues and concerns as mentioned in your answer to Task 4 above.

For the purposes of this exercise, avoid discussions about using "certificate-based authentication", "https protocol" and "encrypting information for communication" purposes.

Task 6. Programming Task [Assume you have completed Task 5 above]

Implement your design in Task 5. Your program should meet the requirements (1-4) listed in Task 3 Case Study. That is to extend EMS so that its employees can manage their own data. That is, the interface includes two parts as below:



localhost:8080/ED-Secure-war/faces/index.xhtml

Secure Company Ltd Home Page

Welcome to our company

We aim at developing secure enterprise application solutions to corporations.

Employee Management System (Amin)

Employee Management System (Employee)

Hints: one approach is to use jdbc realm (see lab_08):

- use employee id and password to access the Employee Management System.
  For 7.1P: you can use plain text password by defining "NONE" for plain password in jdbc Realm
  For 7.2C (credit task): you should use "SHA-256" for encrypted password

Another approach is to use file realm:

- Let the user to use ed-admin1/ed-user1 to get into the main menu for employees, then use employee id and password to access the employee.
  tip: e.g. for ed-user1, use employee id (empId) and password
  use: Employee employee = employeeFacade.find(empId);
  check: employee.getAppGroup().equals("ED-APP-USERS")
  employee.getPassword().equals(pwd))

Task 7. Testing [Assume you have completed Task 6 above]

Write your test cases (including the database content and input values) and test your work thoroughly. You should test the user in the *ED-APP-USERS* group cannot login in the Employee Management System (Admin), i.e. Authorization Failure Page will be shown up.

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 practical class. You should be able to do this and explain your code when asked in the practical session.