StuDocu.com

Lab 7 Pass Task - Lab 7 Pass Task

COS30041 Creating Secure and Scalable Software (Swinburne University of Technology)

StuDocu is not sponsored or endorsed by any college or university
Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

COS 30041 Creating Secure & Scalable Software

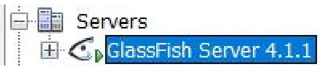
Lab 07 Pass Task

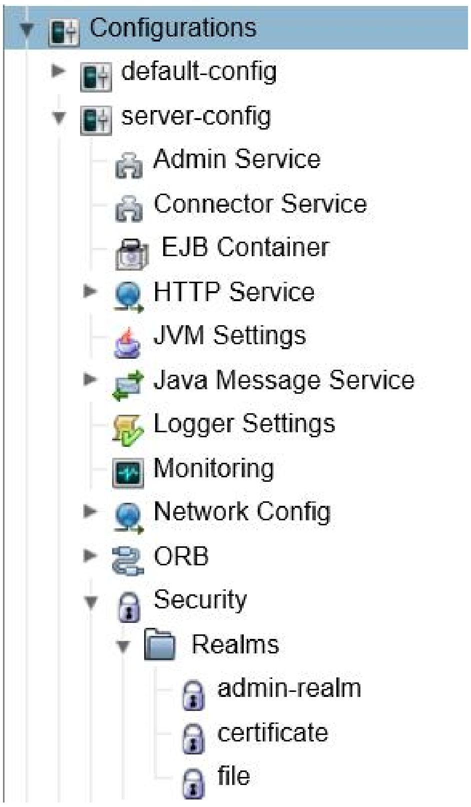
Name: Jason Goh Wei Ting

ID: 101210787

Tutor: Dr. Brian Loh

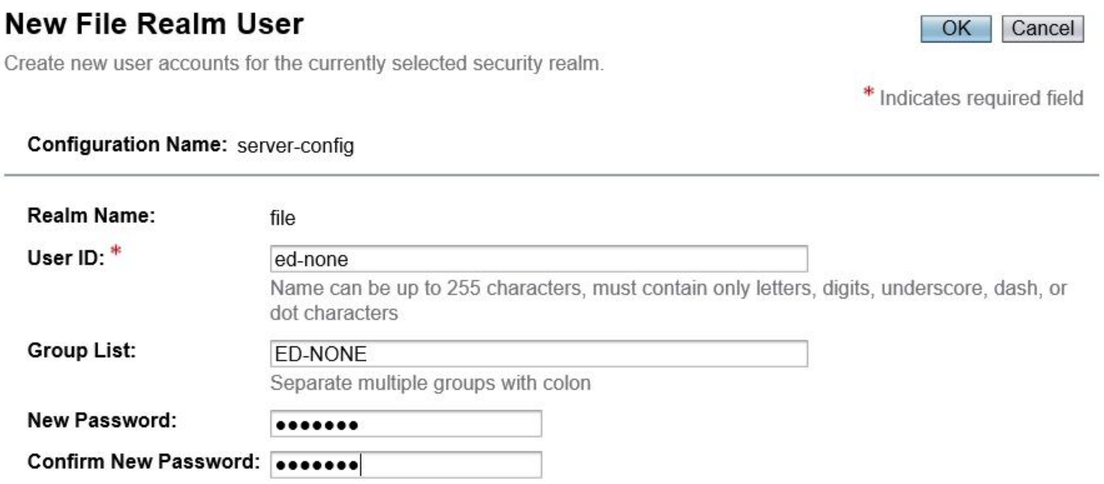
Task 1





This document is available free of charge on StuDocu.com

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)



New File Realm User

Create new user accounts for the currently selected security realm.

* Indicates required field

Configuration Name: server-config

Realm Name: file

User ID: * ed-none

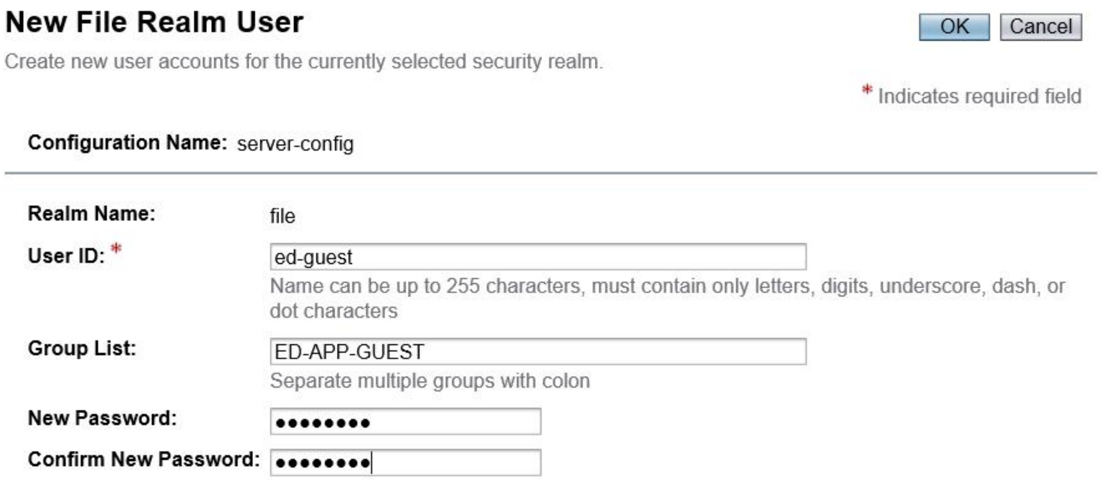
Name can be up to 255 characters, must contain only letters, digits, underscore, dash, or dot characters

Group List: ED-NONE

Separate multiple groups with colon

New Password: ●●●●●●●

Confirm New Password: ●●●●●●●



New File Realm User

Create new user accounts for the currently selected security realm.

* Indicates required field

Configuration Name: server-config

Realm Name: file

User ID: * ed-guest

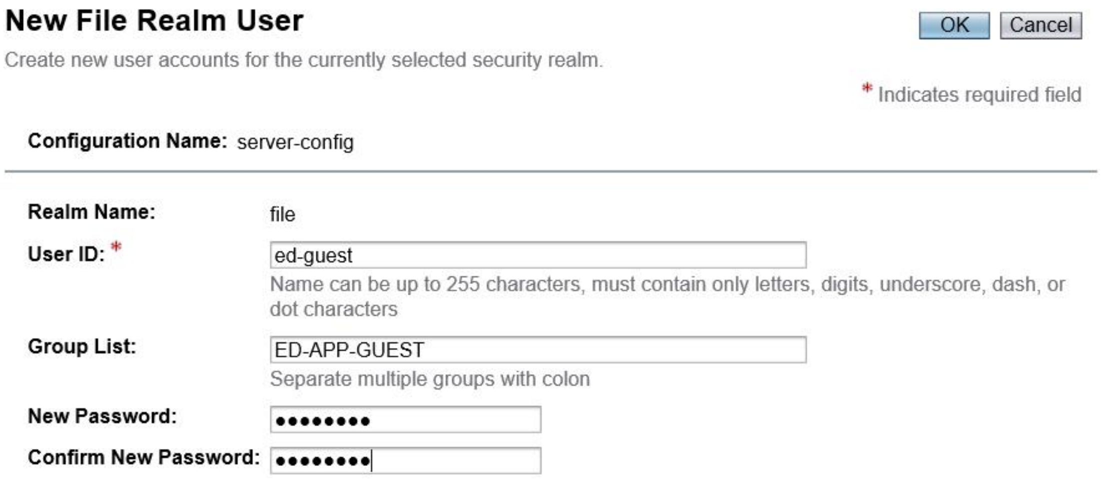
Name can be up to 255 characters, must contain only letters, digits, underscore, dash, or dot characters

Group List: ED-APP-GUEST

Separate multiple groups with colon

New Password: ●●●●●●●●

Confirm New Password: ●●●●●●●●



New File Realm User

Create new user accounts for the currently selected security realm.

* Indicates required field

Configuration Name: server-config

Realm Name: file

User ID: * ed-guest

Name can be up to 255 characters, must contain only letters, digits, underscore, dash, or dot characters

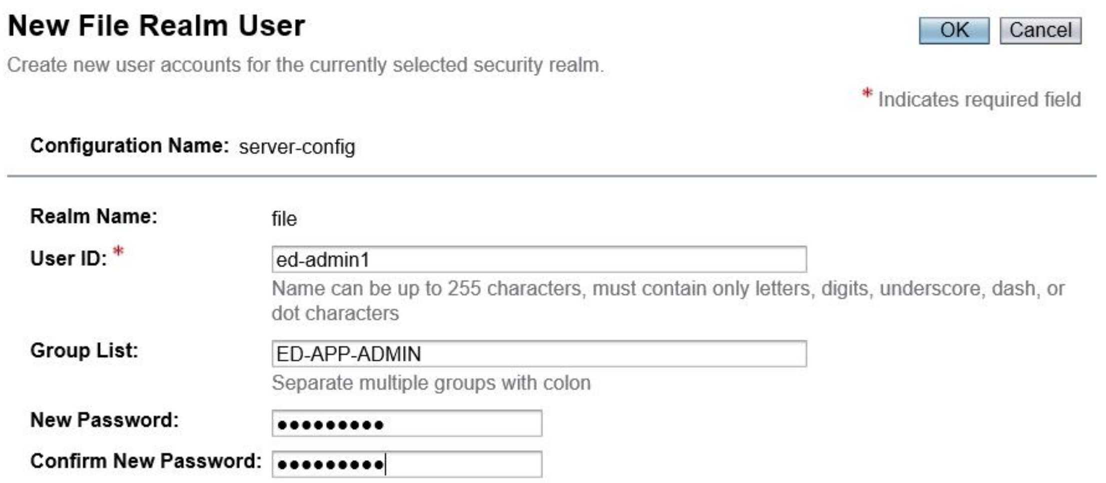
Group List: ED-APP-GUEST

Separate multiple groups with colon

New Password: ●●●●●●●●

Confirm New Password: ●●●●●●●●

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)



New File Realm User

Create new user accounts for the currently selected security realm.

* Indicates required field

Configuration Name: server-config

Realm Name: file

User ID: * ed-admin1

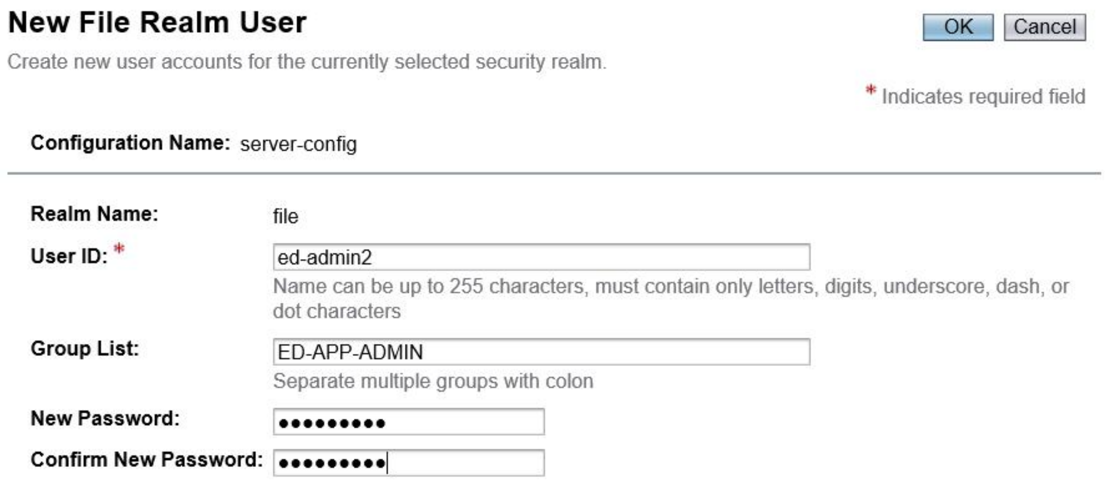
Name can be up to 255 characters, must contain only letters, digits, underscore, dash, or dot characters

Group List: ED-APP-ADMIN

Separate multiple groups with colon

New Password: ●●●●●●●●●

Confirm New Password: ●●●●●●●●●



New File Realm User

Create new user accounts for the currently selected security realm.

* Indicates required field

Configuration Name: server-config

Realm Name: file

User ID: * ed-admin2

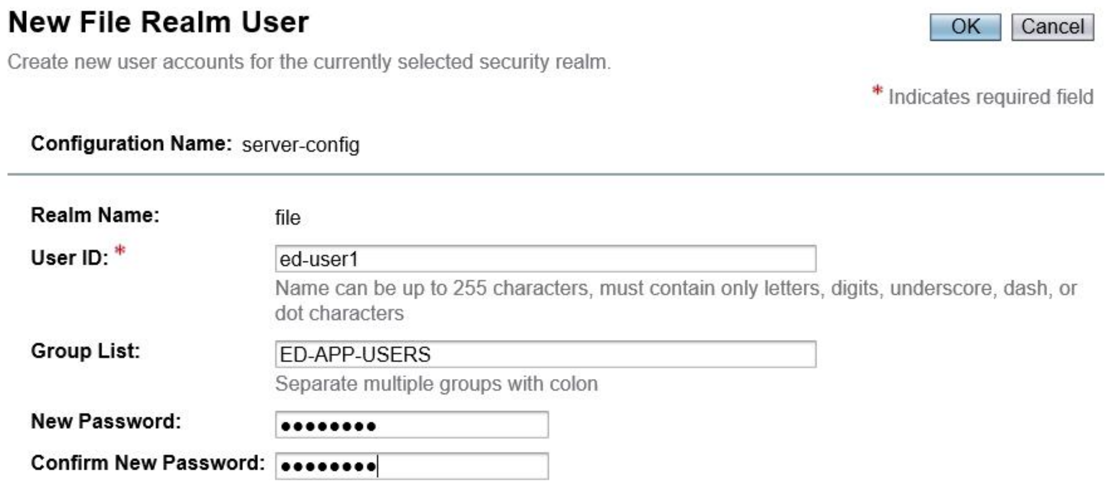
Name can be up to 255 characters, must contain only letters, digits, underscore, dash, or dot characters

Group List: ED-APP-ADMIN

Separate multiple groups with colon

New Password: ●●●●●●●●●

Confirm New Password: ●●●●●●●●●



New File Realm User

Create new user accounts for the currently selected security realm.

* Indicates required field

Configuration Name: server-config

Realm Name: file

User ID: * ed-user1

Name can be up to 255 characters, must contain only letters, digits, underscore, dash, or dot characters

Group List: ED-APP-USERS

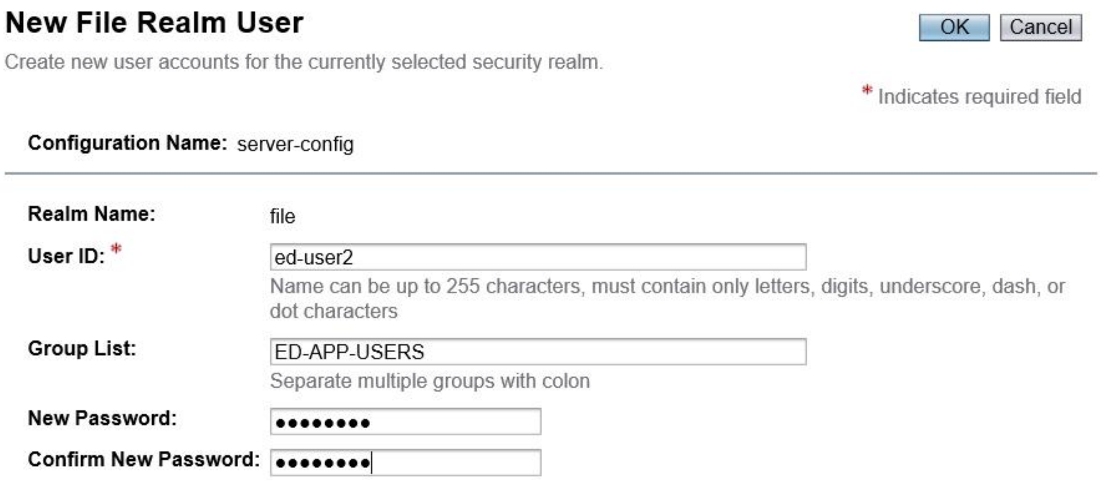
Separate multiple groups with colon

New Password: ●●●●●●●●

Confirm New Password: ●●●●●●●●

This document is available free of charge on StuDocu.com

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)



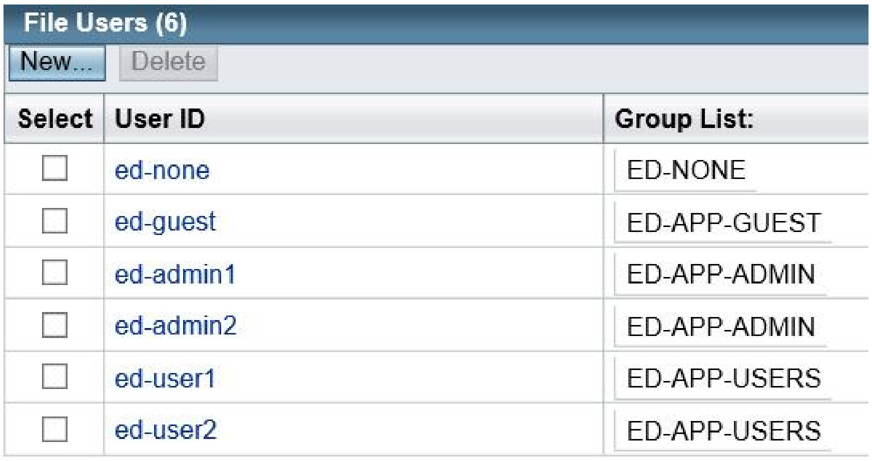
New File Realm User

Create new user accounts for the currently selected security realm.

* Indicates required field

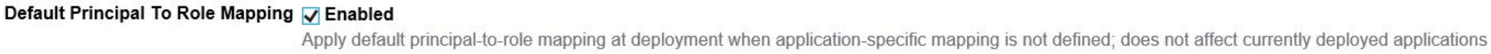
Configuration Name: server-config

Realm Name:	file
User ID: *	ed-user2 Name can be up to 255 characters, must contain only letters, digits, underscore, dash, or dot characters
Group List:	ED-APP-USERS Separate multiple groups with colon
New Password:	••••••••
Confirm New Password:	••••••••



File Users (6)

Select	User ID	Group List:
□	ed-none	ED-NONE
□	ed-guest	ED-APP-GUEST
□	ed-admin1	ED-APP-ADMIN
□	ed-admin2	ED-APP-ADMIN
□	ed-user1	ED-APP-USERS
□	ed-user2	ED-APP-USERS

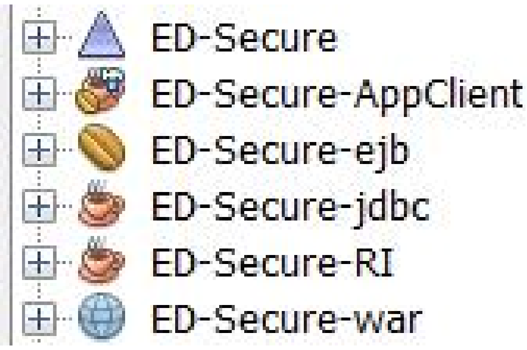


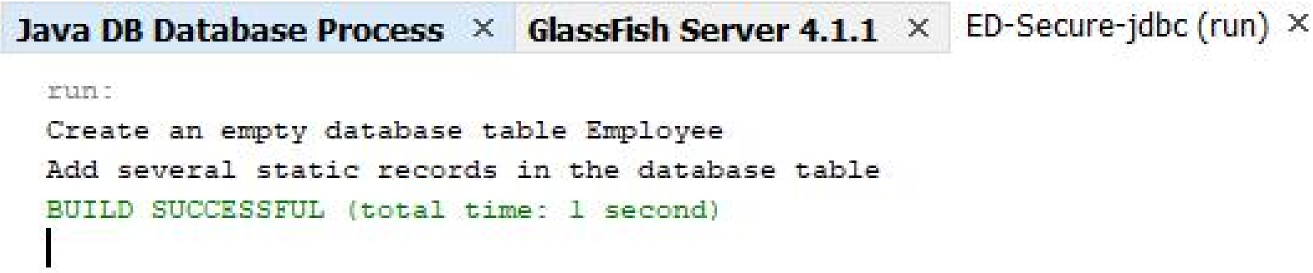
Default Principal To Role Mapping ☑ **Enabled**

Apply default principal-to-role mapping at deployment when application-specific mapping is not defined; does not affect currently deployed applications

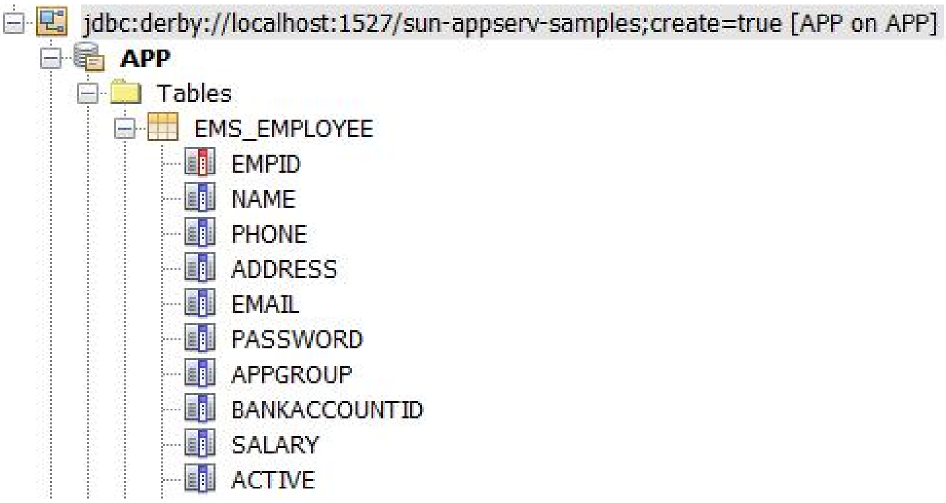
Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

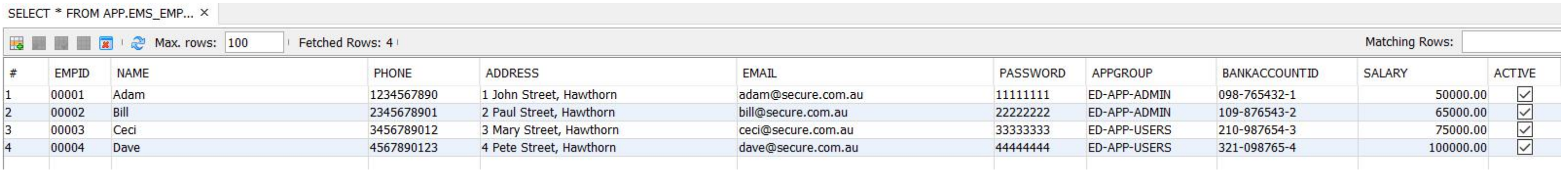
Task 2





```
run:
Create an empty database table Employee
Add several static records in the database table
BUILD SUCCESSFUL (total time: 1 second)
```

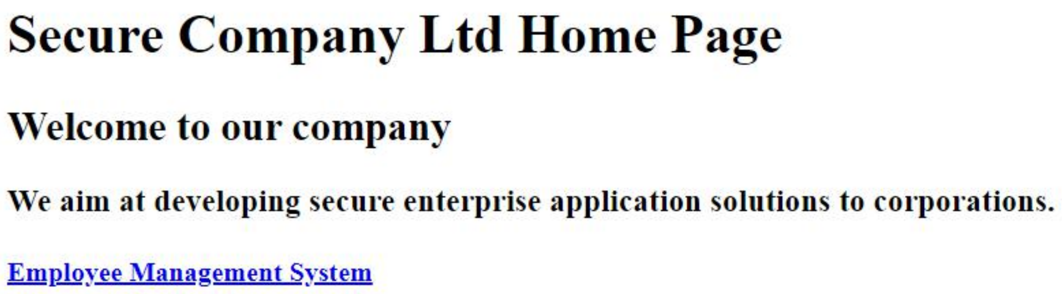




#	EMPID	NAME	PHONE	ADDRESS	EMAIL	PASSWORD	APPGROUP	BANKACCOUNTID	SALARY	ACTIVE
1	00001	Adam	1234567890	1 John Street, Hawthorn	adam@secure.com.au	11111111	ED-APP-ADMIN	098-765432-1	50000.00	☑
2	00002	Bill	2345678901	2 Paul Street, Hawthorn	bill@secure.com.au	22222222	ED-APP-ADMIN	109-876543-2	65000.00	☑
3	00003	Ceci	3456789012	3 Mary Street, Hawthorn	ceci@secure.com.au	33333333	ED-APP-USERS	210-987654-3	75000.00	☑
4	00004	Dave	4567890123	4 Pete Street, Hawthorn	dave@secure.com.au	44444444	ED-APP-USERS	321-098765-4	100000.00	☑

This document is available free of charge on StuDocu.com

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

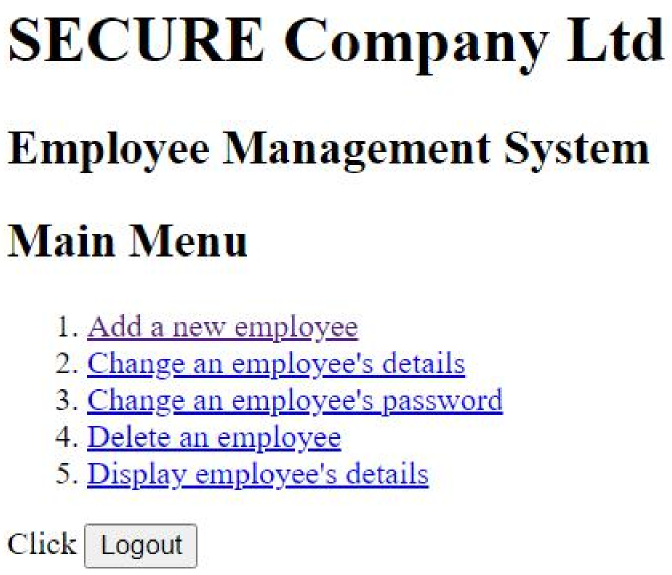


Secure Company Ltd Home Page

Welcome to our company

We aim at developing secure enterprise application solutions to corporations.

Employee Management System



SECURE Company Ltd

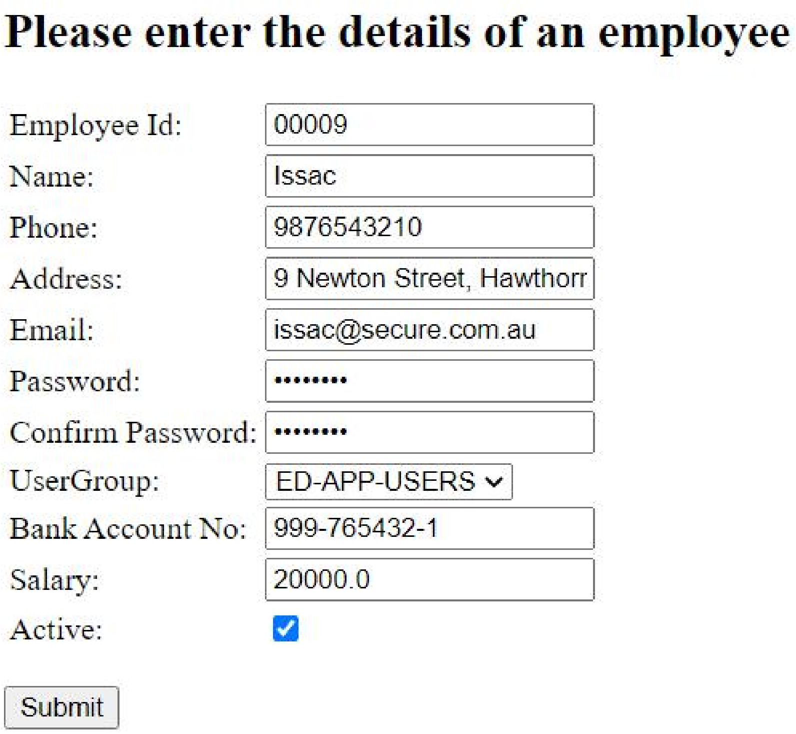
Employee Management System

Main Menu

1. Add a new employee
2. Change an employee's details
3. Change an employee's password
4. Delete an employee
5. Display employee's details

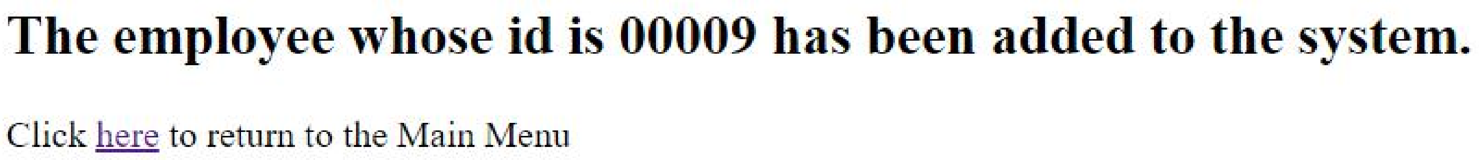
Click

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)



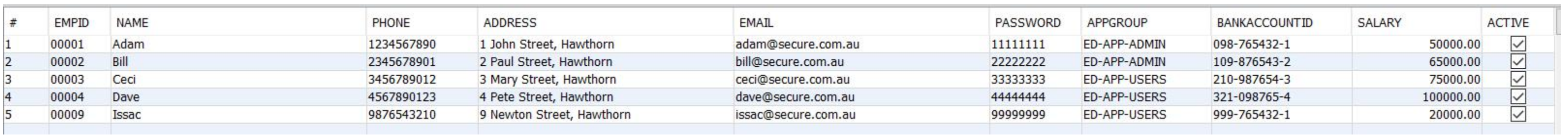
Please enter the details of an employee

Employee Id:	00009
Name:	Issac
Phone:	9876543210
Address:	9 Newton Street, Hawthorr
Email:	issac@secure.com.au
Password:	••••••••
Confirm Password:	••••••••
UserGroup:	ED-APP-USERS
Bank Account No:	999-765432-1
Salary:	20000.0
Active:	☑

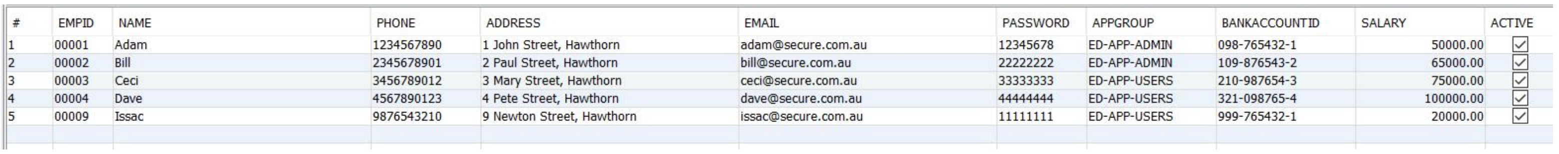


The employee whose id is 00009 has been added to the system.

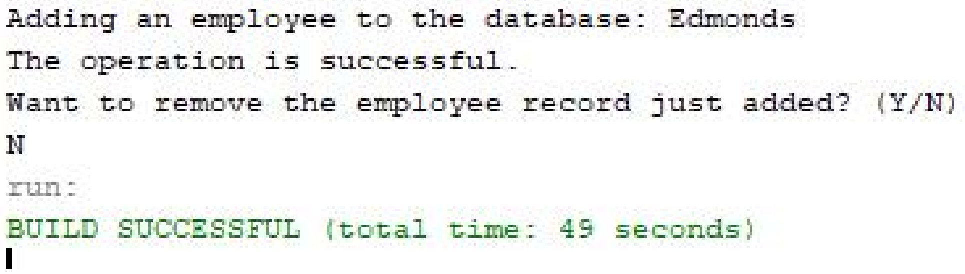
Click here to return to the Main Menu



#	EMPID	NAME	PHONE	ADDRESS	EMAIL	PASSWORD	APPGROUP	BANKACCOUNTID	SALARY	ACTIVE
1	00001	Adam	1234567890	1 John Street, Hawthorn	adam@secure.com.au	11111111	ED-APP-ADMIN	098-765432-1	50000.00	☑
2	00002	Bill	2345678901	2 Paul Street, Hawthorn	bill@secure.com.au	22222222	ED-APP-ADMIN	109-876543-2	65000.00	☑
3	00003	Ceci	3456789012	3 Mary Street, Hawthorn	ceci@secure.com.au	33333333	ED-APP-USERS	210-987654-3	75000.00	☑
4	00004	Dave	4567890123	4 Pete Street, Hawthorn	dave@secure.com.au	44444444	ED-APP-USERS	321-098765-4	100000.00	☑
5	00009	Issac	9876543210	9 Newton Street, Hawthorn	issac@secure.com.au	99999999	ED-APP-USERS	999-765432-1	20000.00	☑



#	EMPID	NAME	PHONE	ADDRESS	EMAIL	PASSWORD	APPGROUP	BANKACCOUNTID	SALARY	ACTIVE
1	00001	Adam	1234567890	1 John Street, Hawthorn	adam@secure.com.au	12345678	ED-APP-ADMIN	098-765432-1	50000.00	☑
2	00002	Bill	2345678901	2 Paul Street, Hawthorn	bill@secure.com.au	22222222	ED-APP-ADMIN	109-876543-2	65000.00	☑
3	00003	Ceci	3456789012	3 Mary Street, Hawthorn	ceci@secure.com.au	33333333	ED-APP-USERS	210-987654-3	75000.00	☑
4	00004	Dave	4567890123	4 Pete Street, Hawthorn	dave@secure.com.au	44444444	ED-APP-USERS	321-098765-4	100000.00	☑
5	00009	Issac	9876543210	9 Newton Street, Hawthorn	issac@secure.com.au	11111111	ED-APP-USERS	999-765432-1	20000.00	☑

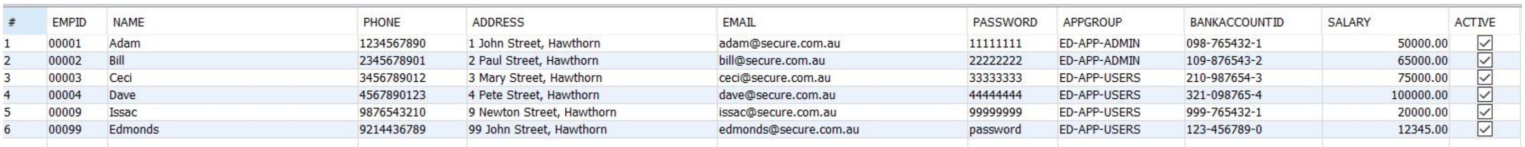


```
Adding an employee to the database: Edmonds
The operation is successful.
Want to remove the employee record just added? (Y/N)
N
run:
BUILD SUCCESSFUL (total time: 49 seconds)
```

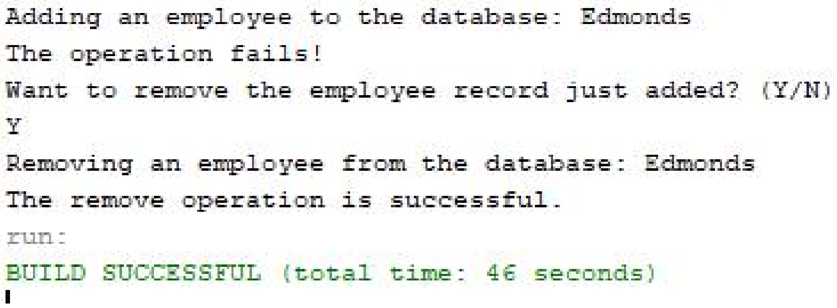
This document is available free of charge on StuDocu.com

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

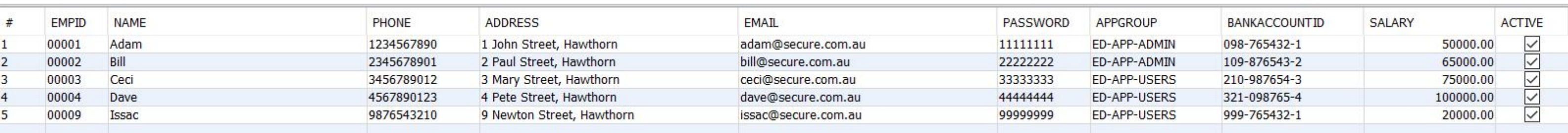
12345.0012



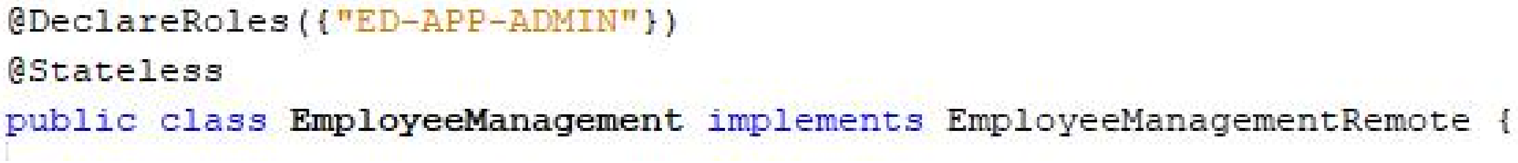
#	EMPID	NAME	PHONE	ADDRESS	EMAIL	PASSWORD	APPGROUP	BANKACCOUNTID	SALARY	ACTIVE
1	00001	Adam	1234567890	1 John Street, Hawthorn	adam@secure.com.au	11111111	ED-APP-ADMIN	098-765432-1	50000.00	☑
2	00002	Bill	2345678901	2 Paul Street, Hawthorn	bill@secure.com.au	22222222	ED-APP-ADMIN	109-876543-2	65000.00	☑
3	00003	Ceci	3456789012	3 Mary Street, Hawthorn	ceci@secure.com.au	33333333	ED-APP-USERS	210-987654-3	75000.00	☑
4	00004	Dave	4567890123	4 Pete Street, Hawthorn	dave@secure.com.au	44444444	ED-APP-USERS	321-098765-4	100000.00	☑
5	00009	Issac	9876543210	9 Newton Street, Hawthorn	issac@secure.com.au	99999999	ED-APP-USERS	999-765432-1	20000.00	☑
6	00099	Edmonds	9214436789	99 John Street, Hawthorn	edmonds@secure.com.au	password	ED-APP-USERS	123-456789-0	12345.00	☑



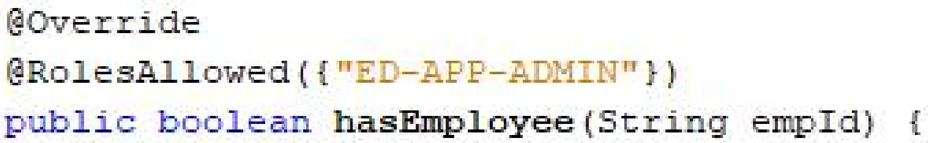
```
Adding an employee to the database: Edmonds
The operation fails!
Want to remove the employee record just added? (Y/N)
Y
Removing an employee from the database: Edmonds
The remove operation is successful.
run:
BUILD SUCCESSFUL (total time: 46 seconds)
```



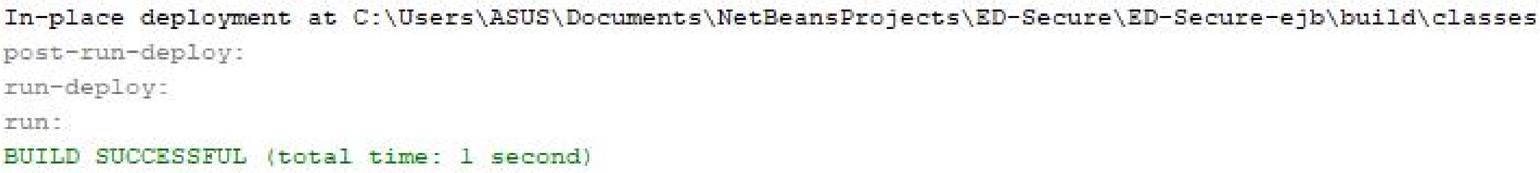
#	EMPID	NAME	PHONE	ADDRESS	EMAIL	PASSWORD	APPGROUP	BANKACCOUNTID	SALARY	ACTIVE
1	00001	Adam	1234567890	1 John Street, Hawthorn	adam@secure.com.au	11111111	ED-APP-ADMIN	098-765432-1	50000.00	☑
2	00002	Bill	2345678901	2 Paul Street, Hawthorn	bill@secure.com.au	22222222	ED-APP-ADMIN	109-876543-2	65000.00	☑
3	00003	Ceci	3456789012	3 Mary Street, Hawthorn	ceci@secure.com.au	33333333	ED-APP-USERS	210-987654-3	75000.00	☑
4	00004	Dave	4567890123	4 Pete Street, Hawthorn	dave@secure.com.au	44444444	ED-APP-USERS	321-098765-4	100000.00	☑
5	00009	Issac	9876543210	9 Newton Street, Hawthorn	issac@secure.com.au	99999999	ED-APP-USERS	999-765432-1	20000.00	☑



```
@DeclareRoles({"ED-APP-ADMIN"})
@Stateless
public class EmployeeManagement implements EmployeeManagementRemote {
```

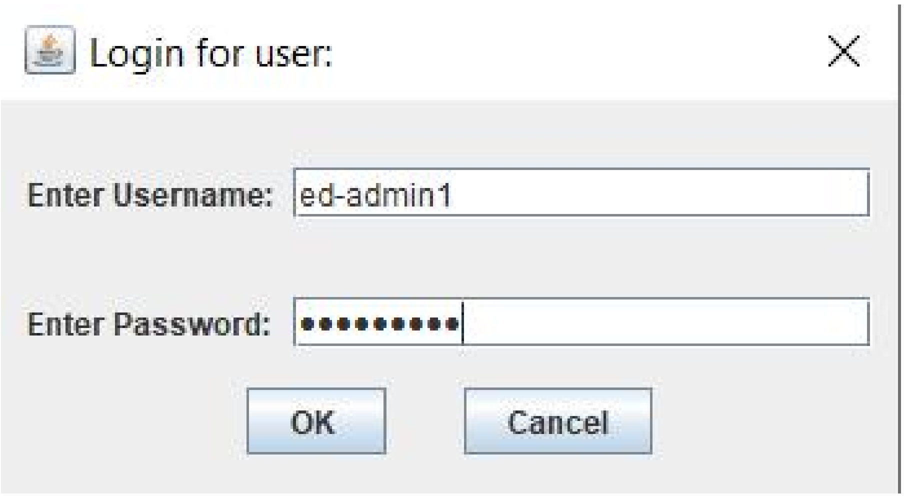


```
@Override
@RolesAllowed({"ED-APP-ADMIN"})
public boolean hasEmployee(String empId) {
```



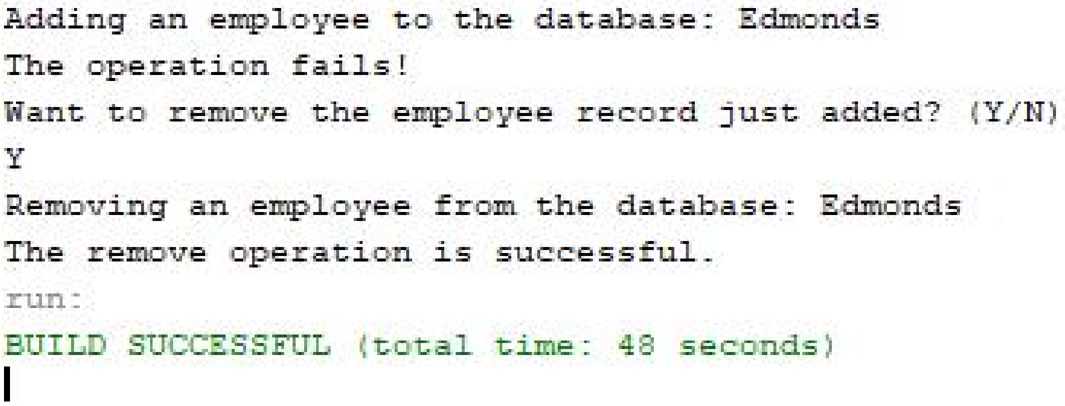
```
In-place deployment at C:\Users\ASUS\Documents\NetBeansProjects\ED-Secure\ED-Secure-ejb\build\classes
post-run-deploy:
run-deploy:
run:
BUILD SUCCESSFUL (total time: 1 second)
```

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

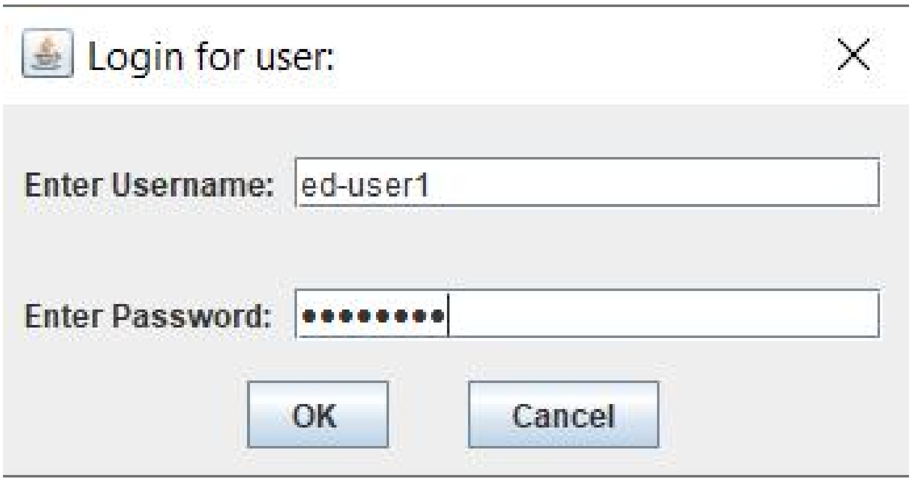


Enter Username: ed-admin1

Enter Password: ●●●●●●●●●●

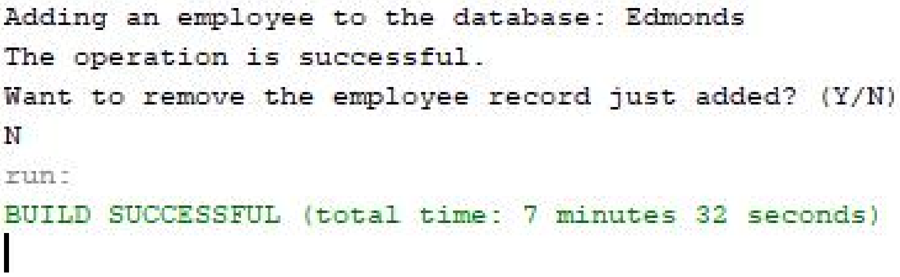


```
Adding an employee to the database: Edmonds
The operation fails!
Want to remove the employee record just added? (Y/N)
Y
Removing an employee from the database: Edmonds
The remove operation is successful.
run:
BUILD SUCCESSFUL (total time: 48 seconds)
```



Enter Username: ed-user1

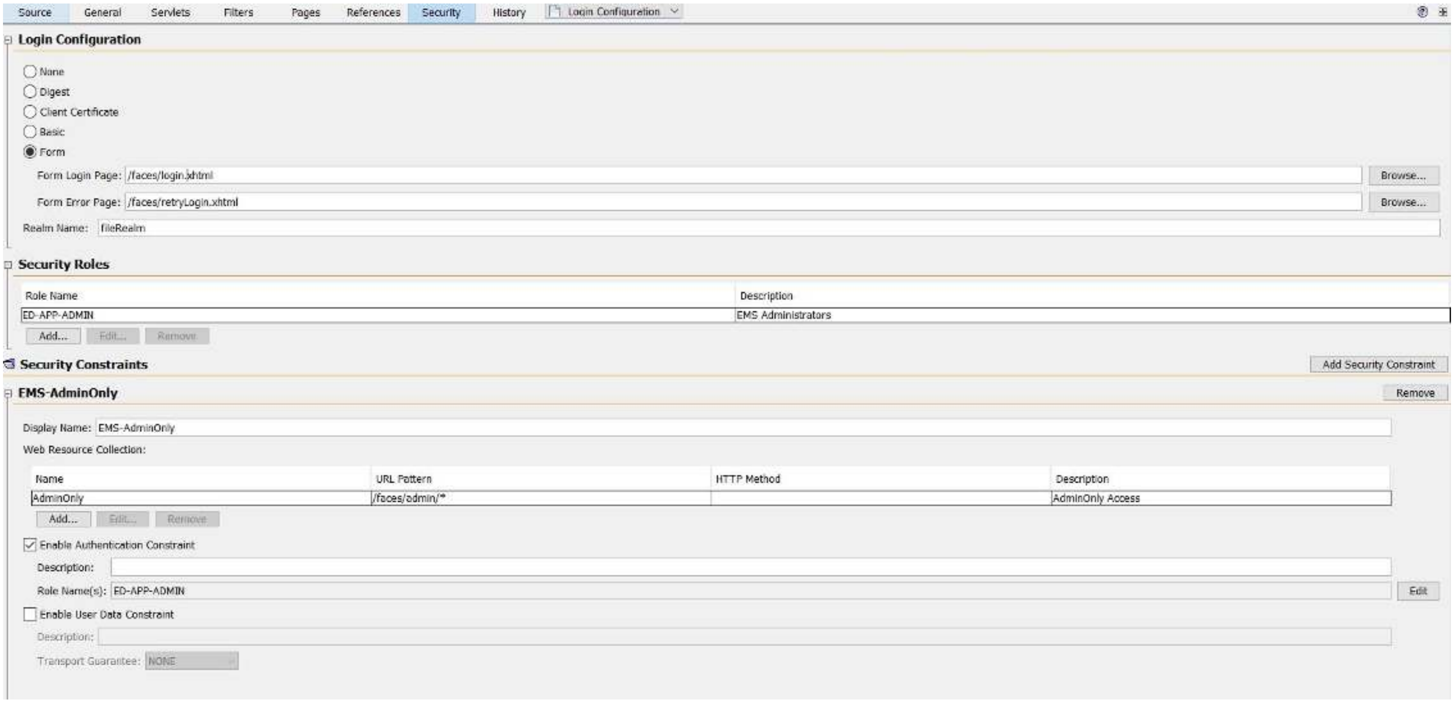
Enter Password: ●●●●●●●●



```
Adding an employee to the database: Edmonds
The operation is successful.
Want to remove the employee record just added? (Y/N)
N
run:
BUILD SUCCESSFUL (total time: 7 minutes 32 seconds)
```

This document is available free of charge on StuDocu.com

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)



Login Configuration

○ None
○ Digest
○ Client Certificate
○ Basic
● Form

Form Login Page: /faces/login.xhtml
Form Error Page: /faces/retryLogin.xhtml
Realm Name: fileRealm

Security Roles

Role Name	Description
ED-APP-ADMIN	EMS Administrators

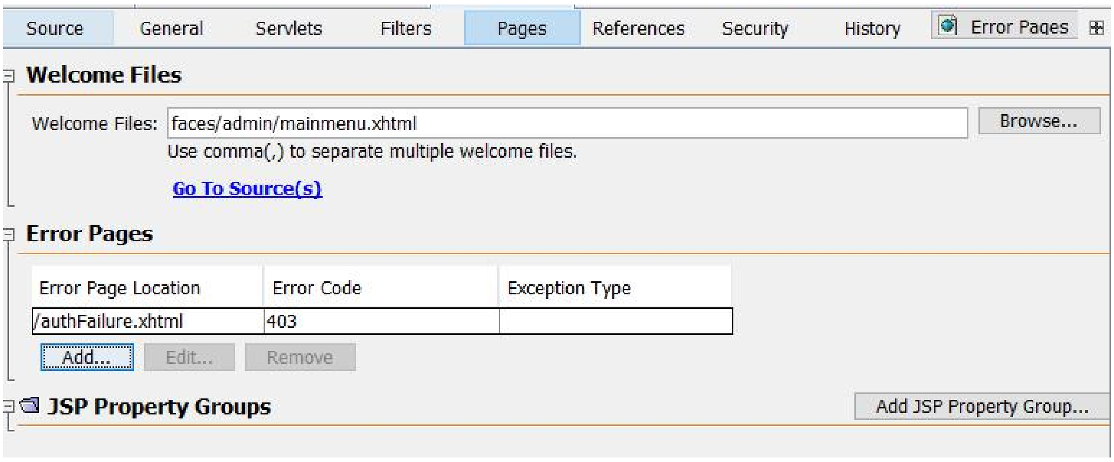
Security Constraints

EMS-AdminOnly

Display Name: EMS-AdminOnly
Web Resource Collection:

Name	URL Pattern	HTTP Method	Description
AdminOnly	/faces/admin/*		AdminOnly Access

☑ Enable Authentication Constraint
Description:
Role Name(s): ED-APP-ADMIN
☐ Enable User Data Constraint
Description:
Transport Guarantee: NONE



Welcome Files

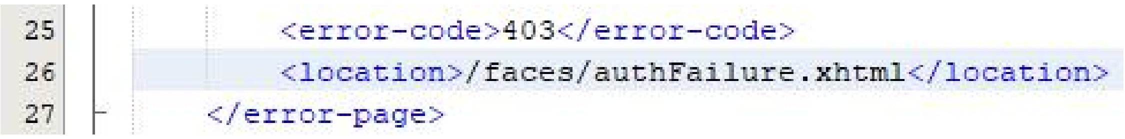
Welcome Files: faces/admin/mainmenu.xhtml
Use comma(,) to separate multiple welcome files.

Go To Source(s)

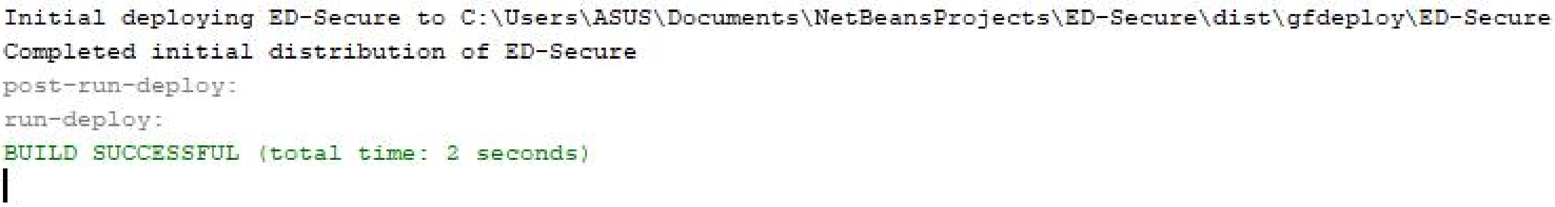
Error Pages

Error Page Location	Error Code	Exception Type
/authFailure.xhtml	403	

JSP Property Groups

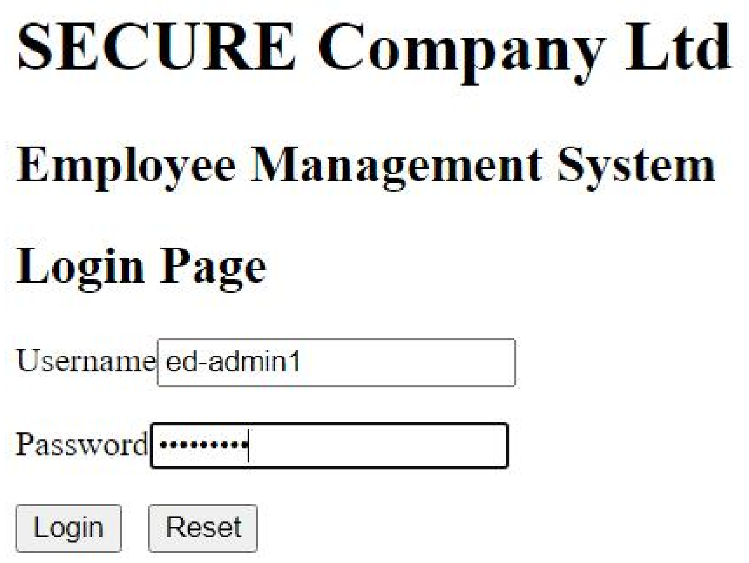


```
            <error-code>403</error-code>
            <location>/faces/authFailure.xhtml</location>
        </error-page>
```



```
Initial deploying ED-Secure to C:\Users\ASUS\Documents\NetBeansProjects\ED-Secure\dist\gfdeploy\ED-Secure
Completed initial distribution of ED-Secure
post-run-deploy:
run-deploy:
BUILD SUCCESSFUL (total time: 2 seconds)
```

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)



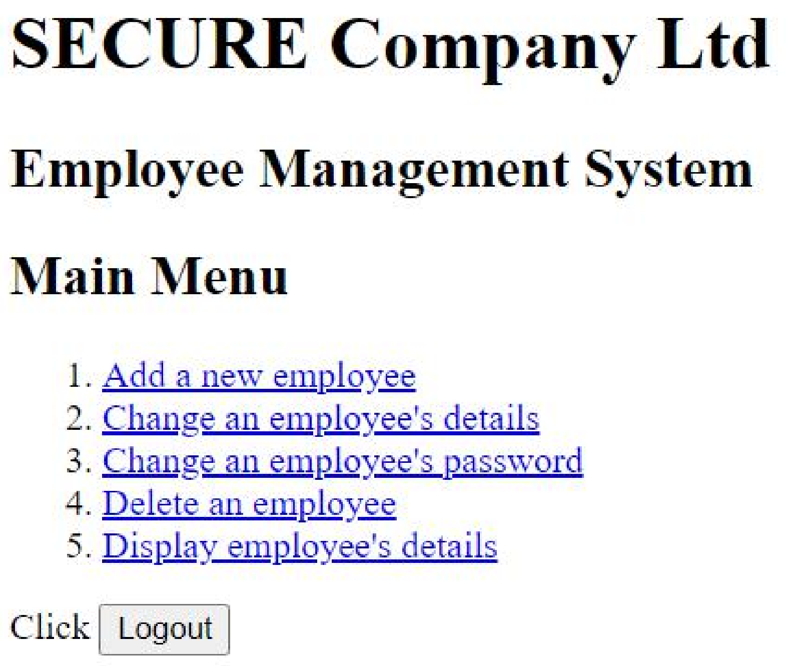
SECURE Company Ltd

Employee Management System

Login Page

Username ed-admin1

Password •••••••••



SECURE Company Ltd

Employee Management System

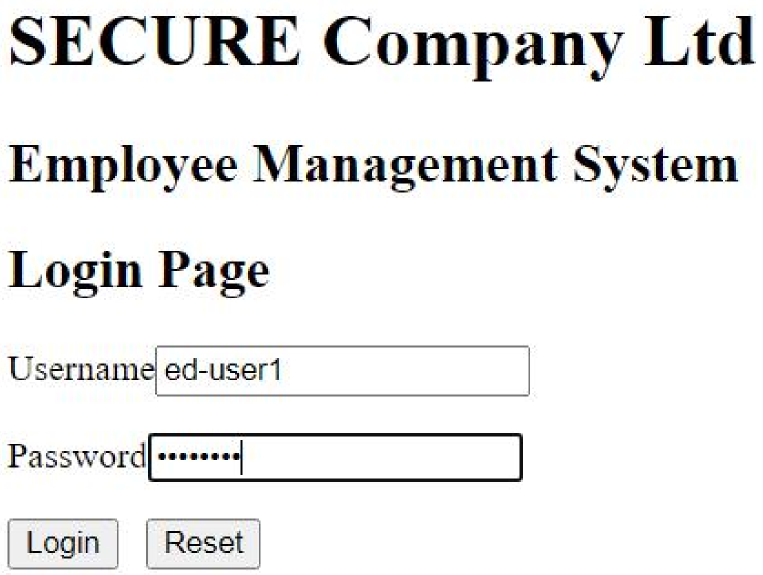
Main Menu

1. Add a new employee
2. Change an employee's details
3. Change an employee's password
4. Delete an employee
5. Display employee's details

Click

This document is available free of charge on StuDocu.com

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)



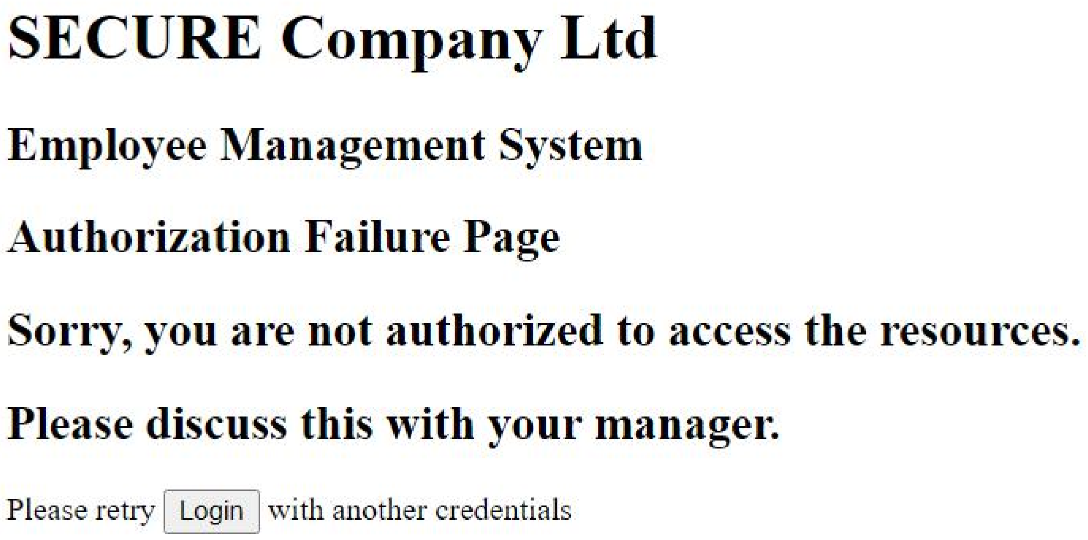
SECURE Company Ltd

Employee Management System

Login Page

Username ed-user1

Password ••••••••



SECURE Company Ltd

Employee Management System

Authorization Failure Page

Sorry, you are not authorized to access the resources.

Please discuss this with your manager.

Please retry Login with another credentials

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

Task 3

Task 4

4.1 - CRUD operations stands for Create, Read, Update and Delete. Employees should not have the permission to perform Create and Delete operations as the function is only available for admin. Admin will be able to create new record and delete existing record. This is to prevent unauthorized personnel from creating records that are not approved by the admin and deleting records might result in data lost of the system. Employees are only allow to either view their record (Read), or edit their record (Update).

4.2 - Employee's review operation is only being able to review their own details excluding password. They will not be able to review other employee's information, this is to keep their personal details private. This is why employees will only be able to review their own details by logging into the system with their unique employee ID and their password, which will never be reviewed by anyone else.

4.3 - The decision on excluding the password being reviewed is a good practice. Password is something that is should be kept as a secret and only known by the password owner itself. Client should not have the permission to gain access to someone else's password, this is to prevent information from being stolen in other possible ways.

4.4

4.4.1 - All information can be updated except for the employee ID. This is because the employee ID is the primary key and is given by the administrator. The employee ID is what the administrator uses to recognise their employees therefore it is not editable. These are not the same as those in 4.2 and 4.3 as to protect their privacy, they are not able to review their password but changing to a new password is allowed but only by the person himself/herself.

This document is available free of charge on StuDocu.com

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

4.4.2 - The employee ID cannot be updated and to avoid it from being updated by accident, employee will not have the option to update their employee ID, it can only be reviewed (Read).

4.5 - The change of the employee's information should occur in the Employee Facade located inside of EIS tier (Business tier). This to ensure that the information updated can also be updated at the same time in the DB server for the employee table.

4.6 - My decision would be to not send the password to the client as it is not safe to be sending the password regardless if it is being displayed or not. If the password is sent but not displayed, it is still possible to decrypt it in some ways. To allow employee to change their own password, they will have to enter their old password first for verifcation. Once their pass the verification, it proves that they are authorized personnel to change the password to a new one.

4.7 - I think that by setting the field "active" to false instead of removing the record from the database is a good practice. This action does not wipe out the employee details entirely from the system. There are a few scenarios where the employee might return to join the company or their details are still needed by the administrators in the future. By setting the field "false" is just a temporary action. This can also protect administrator from removing employees by accident. It can be restored anytime if accident happens.

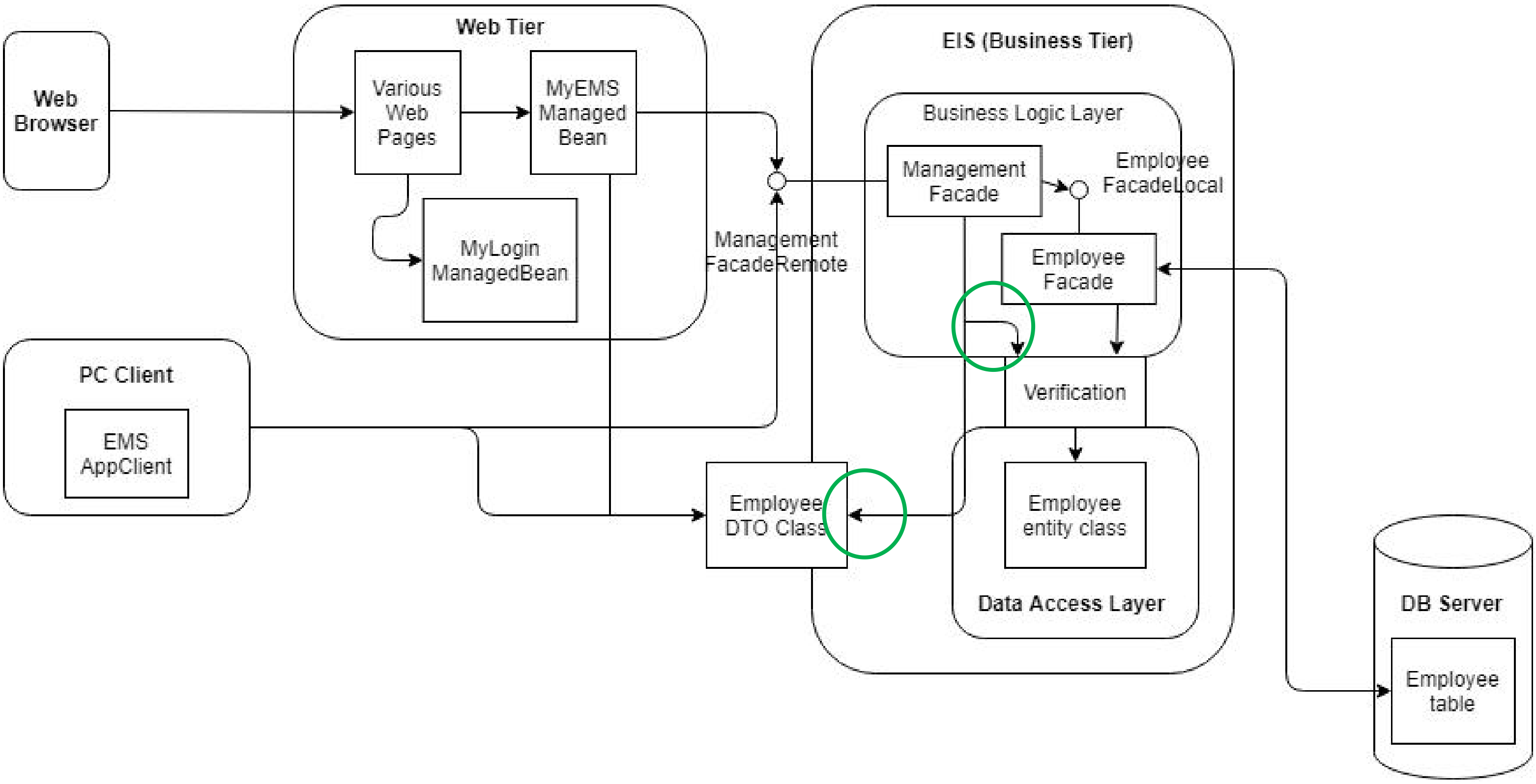
4.8 - After reviewing the features provided, I think that the application will be able to provide the features listed in the Case Study Section above. This is because administrators will be able to perform all CRUD operations while employees can perform C & D operations. For Read operation, employees will only be able to review their own information and password will not be available for review, this is to protect their privacy. On the other hand, for update operation, the employee ID will not be able to be updated while other information can be. Delete operation will only set the field to "false" and not removing it from the database. The only deficiency is that if one's password was stolen and they will be able to use the stolen password to change the

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

password of the account that does not belong to him/her. Perhaps a two-factor authentication can be implemented such as receiving emails or text messages to remind the employee when their password is changed. This is at least inform them that their password had been changed. If they are sure that they did not do it, they can take action immediately to prevent information from being stolen.

Task 5

a.



b. The user uses web browser to gain access to various webpages which are in the Web Tier. Web tier handles the interaction between client and the business tier. It only allow different user role to login into different webpage to perform different actions. In the business tier, the Management Facade is used to transfer data between DAO and DTO (labelled in green). The change of information occurring in Employee Facade allows direct access to the employee table in the DB server. The data access layer keeps the code that is

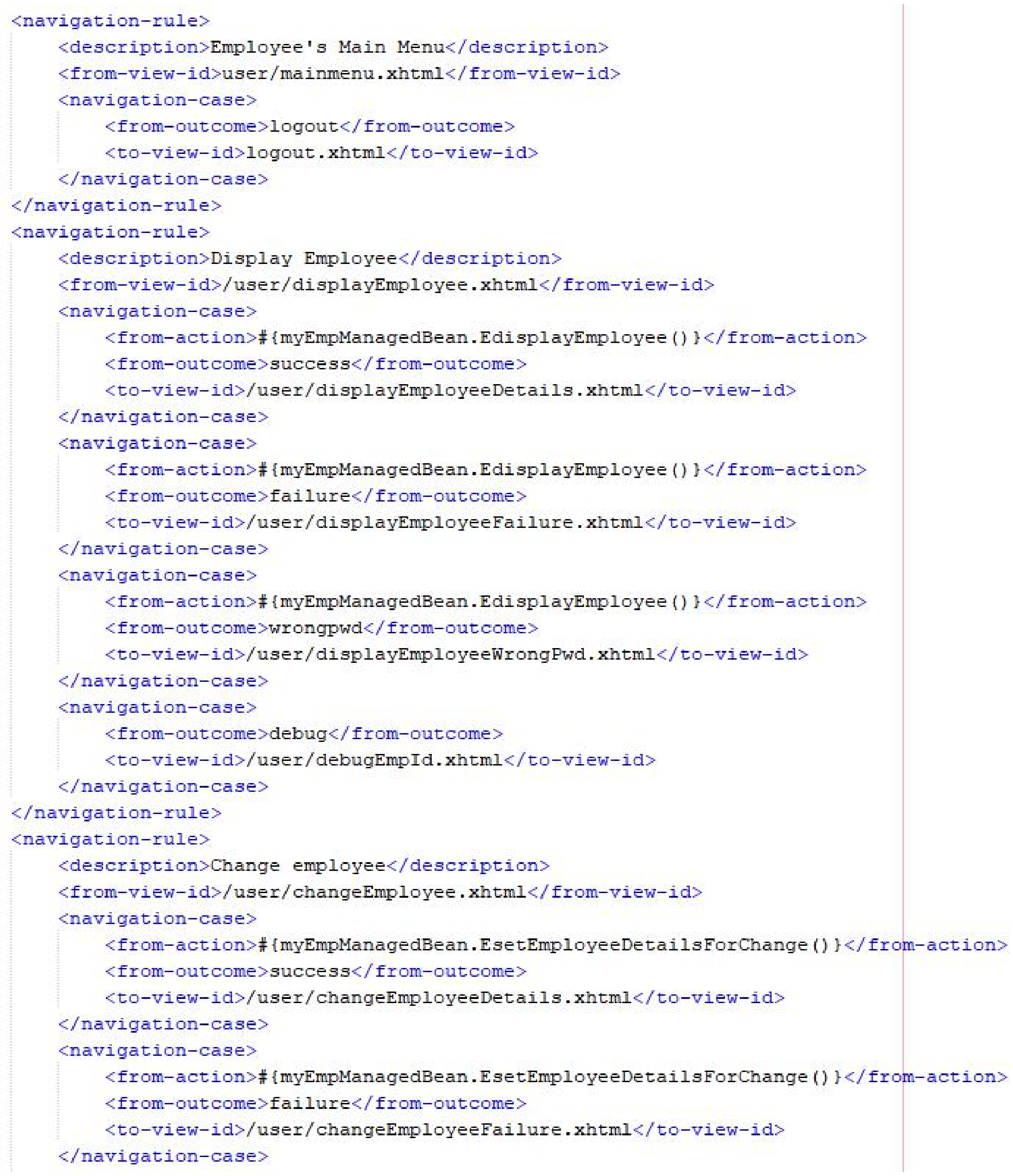
This document is available free of charge on StuDocu.com
Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

used to pull data stored in the DB which is separated from the business logic layer. To be able to access the information, it will need to pass the verfication by using the employee ID and password for privacy protection.

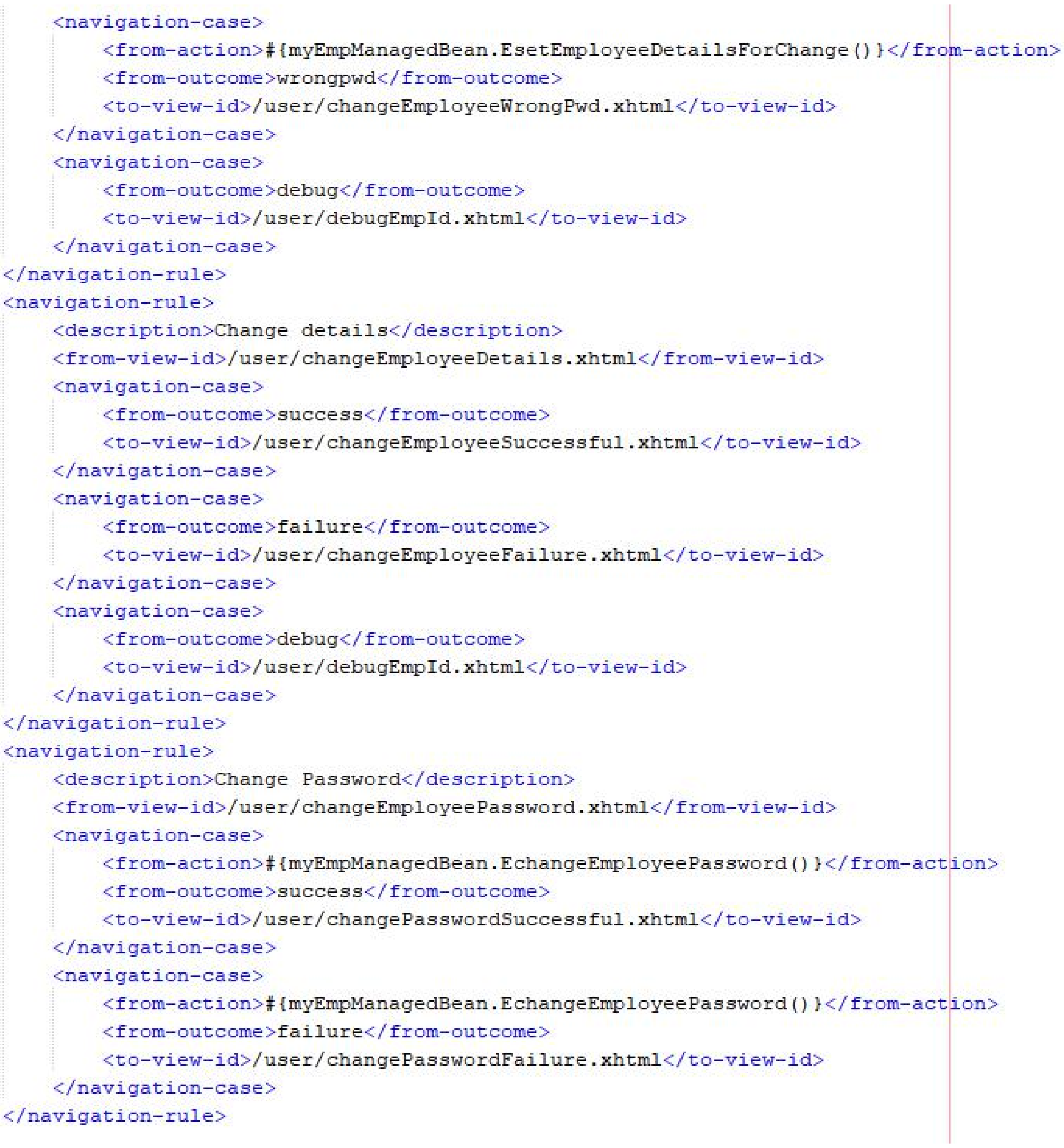
Task 6

- **faces-config.xml**

- newly added navigation rules for user role



```
<navigation-rule>
    <description>Employee's Main Menu</description>
    <from-view-id>user/mainmenu.xhtml</from-view-id>
    <navigation-case>
        <from-outcome>logout</from-outcome>
        <to-view-id>logout.xhtml</to-view-id>
    </navigation-case>
</navigation-rule>
<navigation-rule>
    <description>Display Employee</description>
    <from-view-id>/user/displayEmployee.xhtml</from-view-id>
    <navigation-case>
        <from-action>#{myEmpManagedBean.EdisplayEmployee()}</from-action>
        <from-outcome>success</from-outcome>
        <to-view-id>/user/displayEmployeeDetails.xhtml</to-view-id>
    </navigation-case>
    <navigation-case>
        <from-action>#{myEmpManagedBean.EdisplayEmployee()}</from-action>
        <from-outcome>failure</from-outcome>
        <to-view-id>/user/displayEmployeeFailure.xhtml</to-view-id>
    </navigation-case>
    <navigation-case>
        <from-action>#{myEmpManagedBean.EdisplayEmployee()}</from-action>
        <from-outcome>wrongpwd</from-outcome>
        <to-view-id>/user/displayEmployeeWrongPwd.xhtml</to-view-id>
    </navigation-case>
    <navigation-case>
        <from-outcome>debug</from-outcome>
        <to-view-id>/user/debugEmpId.xhtml</to-view-id>
    </navigation-case>
</navigation-rule>
<navigation-rule>
    <description>Change employee</description>
    <from-view-id>/user/changeEmployee.xhtml</from-view-id>
    <navigation-case>
        <from-action>#{myEmpManagedBean.EsetEmployeeDetailsForChange()}</from-action>
        <from-outcome>success</from-outcome>
        <to-view-id>/user/changeEmployeeDetails.xhtml</to-view-id>
    </navigation-case>
    <navigation-case>
        <from-action>#{myEmpManagedBean.EsetEmployeeDetailsForChange()}</from-action>
        <from-outcome>failure</from-outcome>
        <to-view-id>/user/changeEmployeeFailure.xhtml</to-view-id>
    </navigation-case>
```

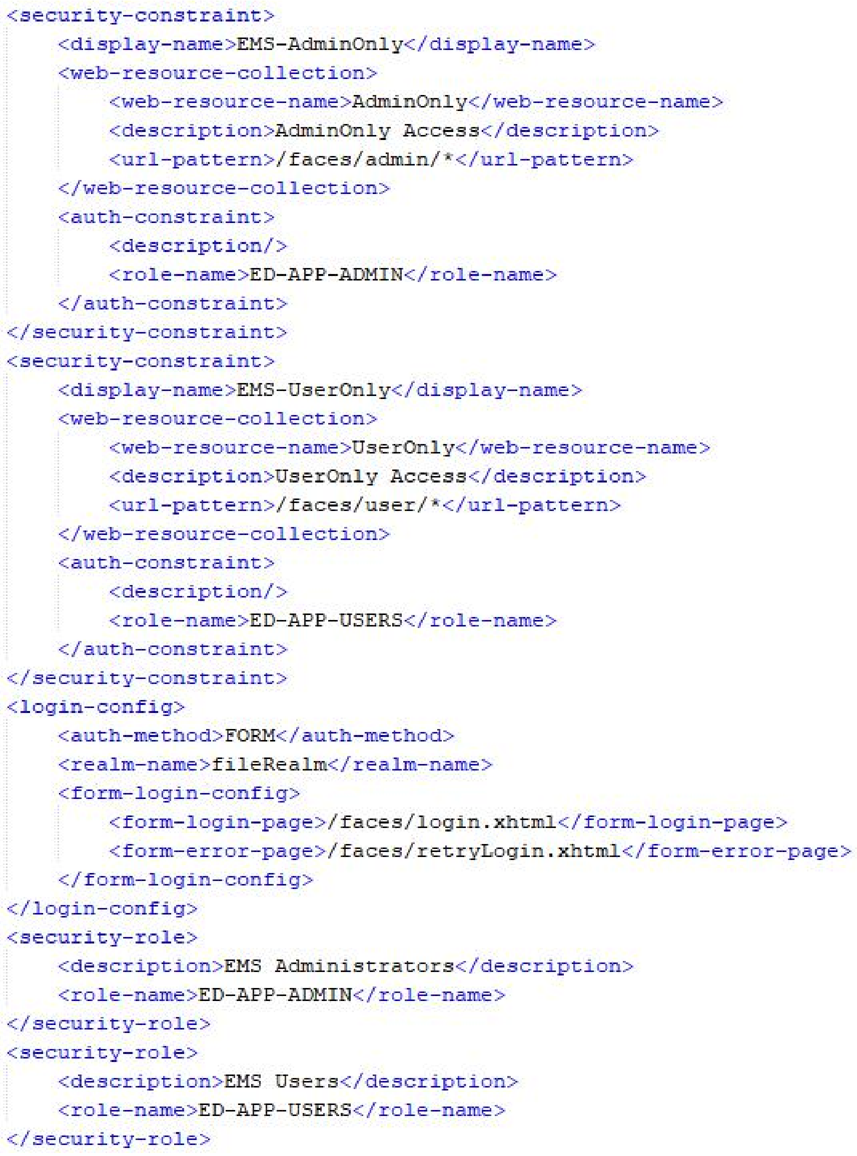


```
    <navigation-case>
        <from-action>#{myEmpManagedBean.EsetEmployeeDetailsForChange()}</from-action>
        <from-outcome>wrongpwd</from-outcome>
        <to-view-id>/user/changeEmployeeWrongPwd.xhtml</to-view-id>
    </navigation-case>
    <navigation-case>
        <from-outcome>debug</from-outcome>
        <to-view-id>/user/debugEmpId.xhtml</to-view-id>
    </navigation-case>
</navigation-rule>
<navigation-rule>
    <description>Change details</description>
    <from-view-id>/user/changeEmployeeDetails.xhtml</from-view-id>
    <navigation-case>
        <from-outcome>success</from-outcome>
        <to-view-id>/user/changeEmployeeSuccessful.xhtml</to-view-id>
    </navigation-case>
    <navigation-case>
        <from-outcome>failure</from-outcome>
        <to-view-id>/user/changeEmployeeFailure.xhtml</to-view-id>
    </navigation-case>
    <navigation-case>
        <from-outcome>debug</from-outcome>
        <to-view-id>/user/debugEmpId.xhtml</to-view-id>
    </navigation-case>
</navigation-rule>
<navigation-rule>
    <description>Change Password</description>
    <from-view-id>/user/changeEmployeePassword.xhtml</from-view-id>
    <navigation-case>
        <from-action>#{myEmpManagedBean.EchangeEmployeePassword()}</from-action>
        <from-outcome>success</from-outcome>
        <to-view-id>/user/changePasswordSuccessful.xhtml</to-view-id>
    </navigation-case>
    <navigation-case>
        <from-action>#{myEmpManagedBean.EchangeEmployeePassword()}</from-action>
        <from-outcome>failure</from-outcome>
        <to-view-id>/user/changePasswordFailure.xhtml</to-view-id>
    </navigation-case>
</navigation-rule>
```

This document is available free of charge on StuDocu.com

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

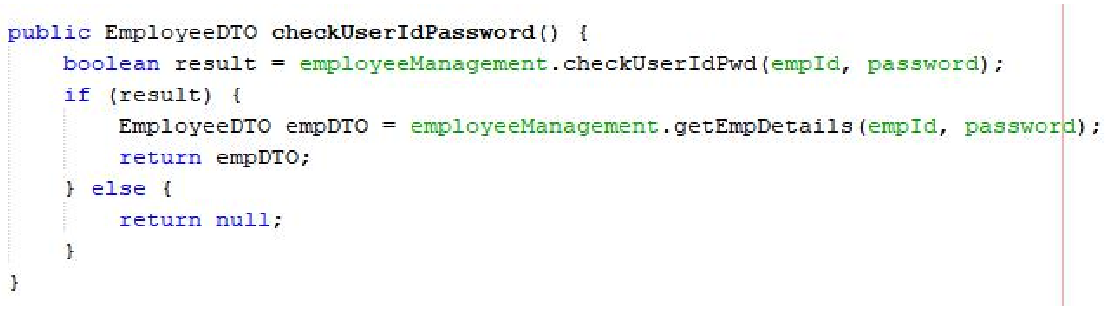
❖ web.xml



```xml
<security-constraint>
    <display-name>EMS-AdminOnly</display-name>
    <web-resource-collection>
        <web-resource-name>AdminOnly</web-resource-name>
        <description>AdminOnly Access</description>
        <url-pattern>/faces/admin/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <description/>
        <role-name>ED-APP-ADMIN</role-name>
    </auth-constraint>
</security-constraint>
<security-constraint>
    <display-name>EMS-UserOnly</display-name>
    <web-resource-collection>
        <web-resource-name>UserOnly</web-resource-name>
        <description>UserOnly Access</description>
        <url-pattern>/faces/user/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <description/>
        <role-name>ED-APP-USERS</role-name>
    </auth-constraint>
</security-constraint>
<login-config>
    <auth-method>FORM</auth-method>
    <realm-name>fileRealm</realm-name>
    <form-login-config>
        <form-login-page>/faces/login.xhtml</form-login-page>
        <form-error-page>/faces/retryLogin.xhtml</form-error-page>
    </form-login-config>
</login-config>
<security-role>
    <description>EMS Administrators</description>
    <role-name>ED-APP-ADMIN</role-name>
</security-role>
<security-role>
    <description>EMS Users</description>
    <role-name>ED-APP-USERS</role-name>
</security-role>
```

❖ myEmpManagedBean.java

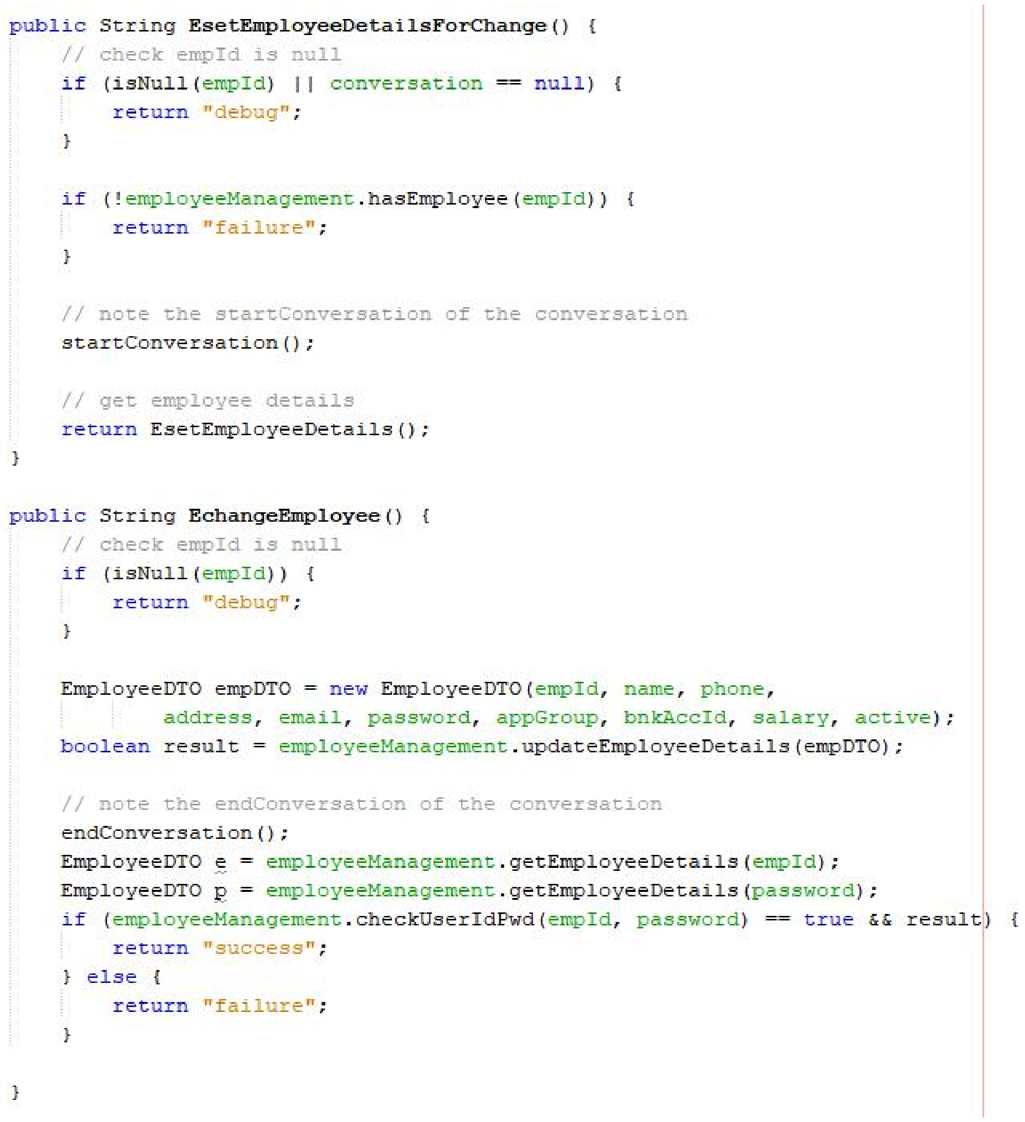
1. checkUserIdPassword()



```java
public EmployeeDTO checkUserIdPassword() {
    boolean result = employeeManagement.checkUserIdPwd(empId, password);
    if (result) {
        EmployeeDTO empDTO = employeeManagement.getEmpDetails(empId, password);
        return empDTO;
    } else {
        return null;
    }
}
```

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

2. Employee Change Details function

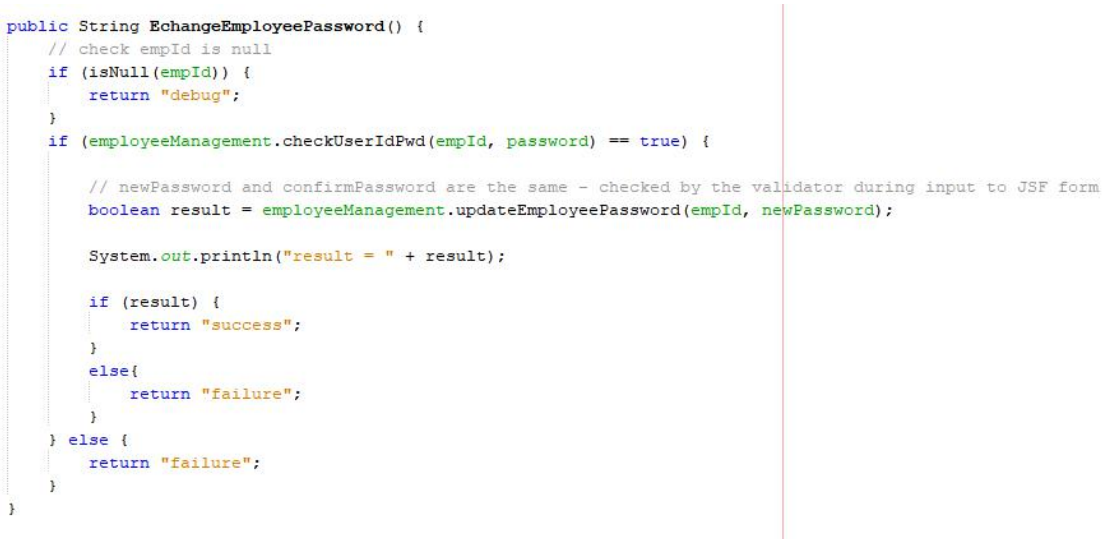


```java
public String EsetEmployeeDetailsForChange() {
    // check empId is null
    if (isNull(empId) || conversation == null) {
        return "debug";
    }

    if (!employeeManagement.hasEmployee(empId)) {
        return "failure";
    }

    // note the startConversation of the conversation
    startConversation();

    // get employee details
    return EsetEmployeeDetails();
}

public String EchangeEmployee() {
    // check empId is null
    if (isNull(empId)) {
        return "debug";
    }

    EmployeeDTO empDTO = new EmployeeDTO(empId, name, phone,
            address, email, password, appGroup, bnkAccId, salary, active);
    boolean result = employeeManagement.updateEmployeeDetails(empDTO);

    // note the endConversation of the conversation
    endConversation();
    EmployeeDTO e = employeeManagement.getEmployeeDetails(empId);
    EmployeeDTO p = employeeManagement.getEmployeeDetails(password);
    if (employeeManagement.checkUserIdPwd(empId, password) == true && result) {
        return "success";
    } else {
        return "failure";
    }

}
```

This document is available free of charge on StuDocu.com

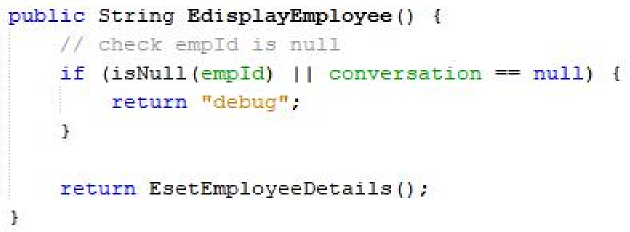
Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

3. Employee Change Password function

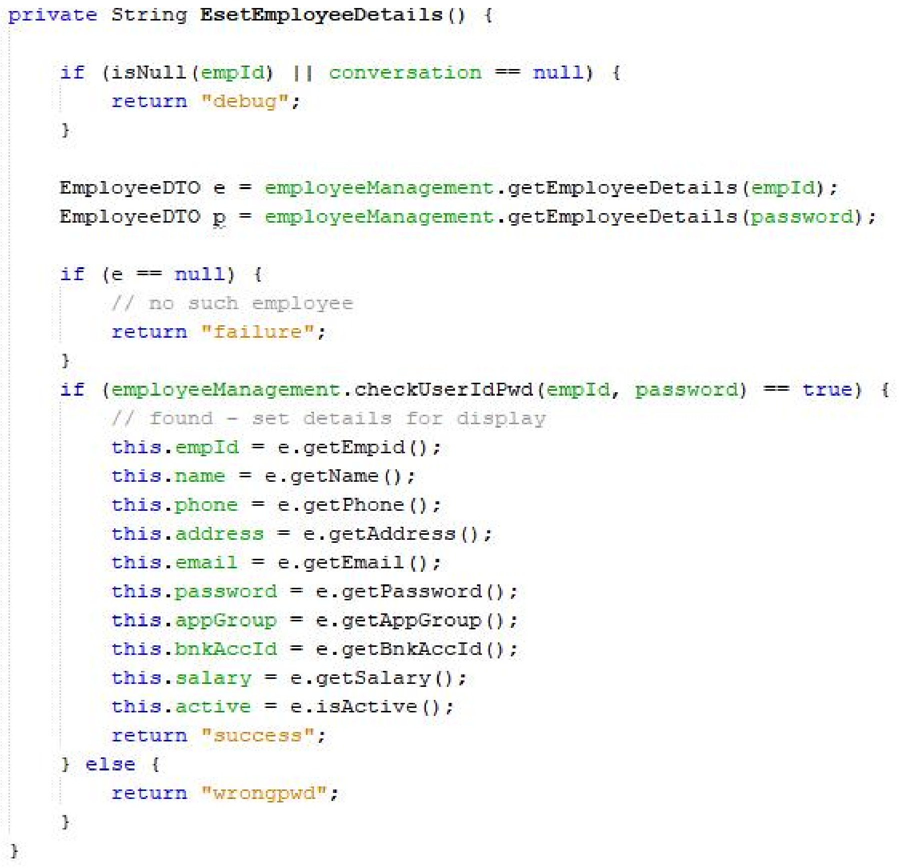


```
public String EchangeEmployeePassword() {
    // check empId is null
    if (isNull(empId)) {
        return "debug";
    }
    if (employeeManagement.checkUserIdPwd(empId, password) == true) {

        // newPassword and confirmPassword are the same - checked by the validator during input to JSF form
        boolean result = employeeManagement.updateEmployeePassword(empId, newPassword);

        System.out.println("result = " + result);

        if (result) {
            return "success";
        }
        else{
            return "failure";
        }
    } else {
        return "failure";
    }
}
```

4. Employee Display Details function



```
public String EdisplayEmployee() {
    // check empId is null
    if (isNull(empId) || conversation == null) {
        return "debug";
    }

    return EsetEmployeeDetails();
}
```

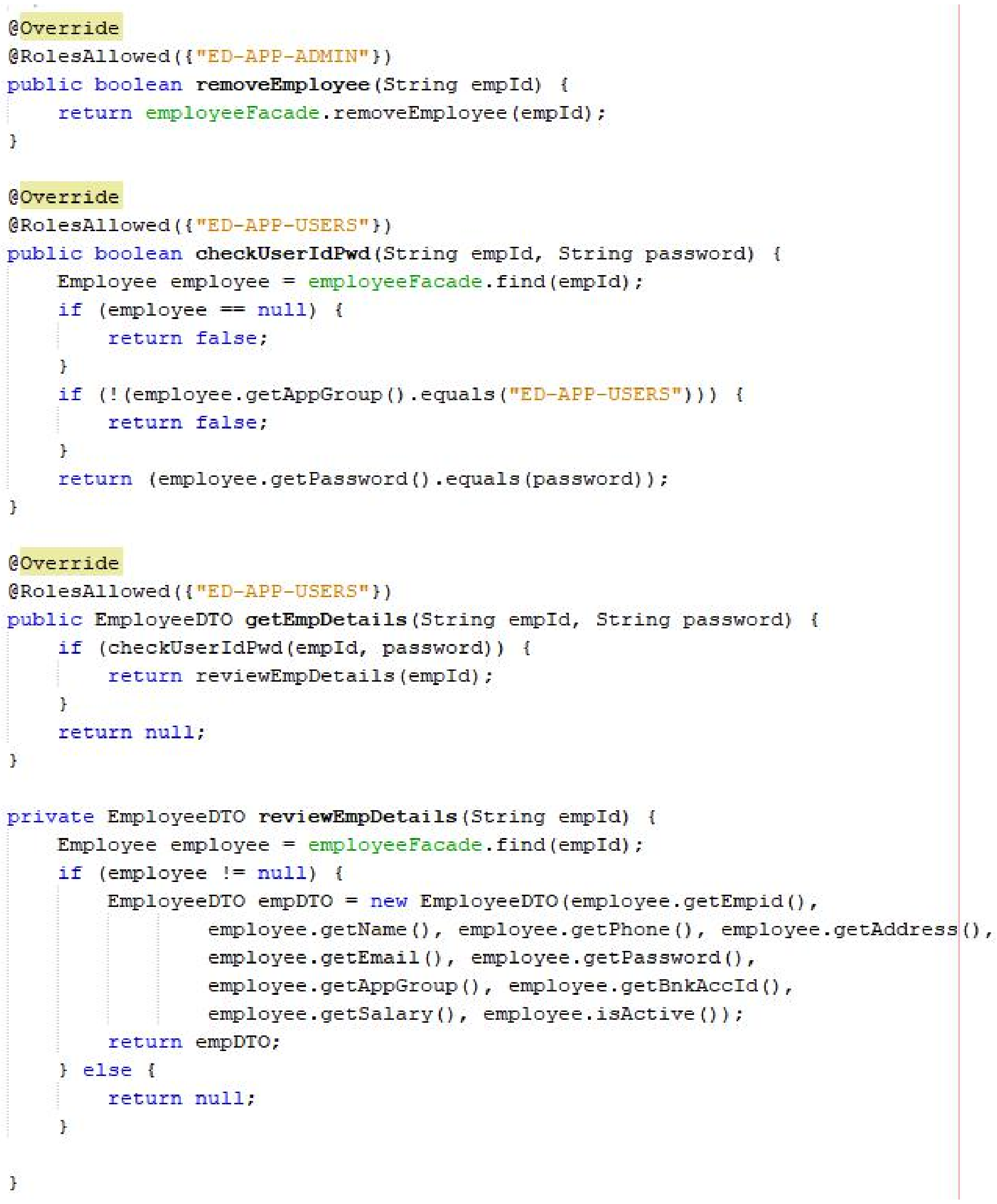


```
private String EsetEmployeeDetails() {

    if (isNull(empId) || conversation == null) {
        return "debug";
    }

    EmployeeDTO e = employeeManagement.getEmployeeDetails(empId);
    EmployeeDTO p = employeeManagement.getEmployeeDetails(password);

    if (e == null) {
        // no such employee
        return "failure";
    }
    if (employeeManagement.checkUserIdPwd(empId, password) == true) {
        // found - set details for display
        this.empId = e.getEmpid();
        this.name = e.getName();
        this.phone = e.getPhone();
        this.address = e.getAddress();
        this.email = e.getEmail();
        this.password = e.getPassword();
        this.appGroup = e.getAppGroup();
        this.bnkAccId = e.getBnkAccId();
        this.salary = e.getSalary();
        this.active = e.isActive();
        return "success";
    } else {
        return "wrongpwd";
    }
}
```

This document is available free of charge on StuDocu.com

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

❖ EmployeeManagement.java

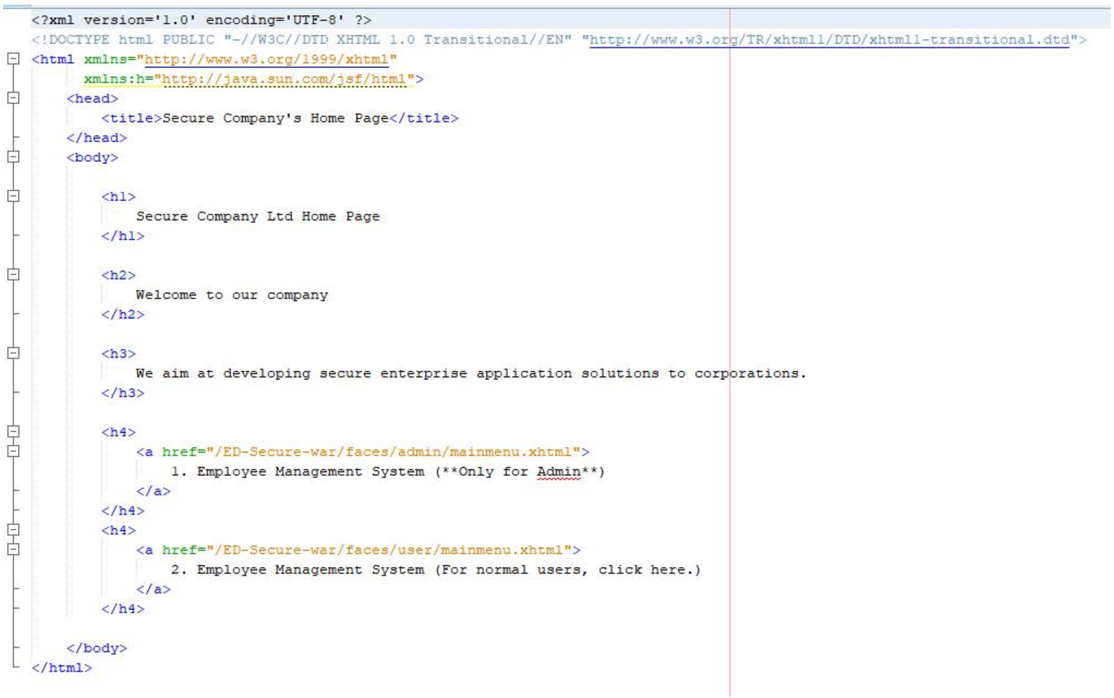


```java
@Override
@RolesAllowed({"ED-APP-ADMIN"})
public boolean removeEmployee(String empId) {
    return employeeFacade.removeEmployee(empId);
}

@Override
@RolesAllowed({"ED-APP-USERS"})
public boolean checkUserIdPwd(String empId, String password) {
    Employee employee = employeeFacade.find(empId);
    if (employee == null) {
        return false;
    }
    if (!(employee.getAppGroup().equals("ED-APP-USERS"))) {
        return false;
    }
    return (employee.getPassword().equals(password));
}

@Override
@RolesAllowed({"ED-APP-USERS"})
public EmployeeDTO getEmpDetails(String empId, String password) {
    if (checkUserIdPwd(empId, password)) {
        return reviewEmpDetails(empId);
    }
    return null;
}

private EmployeeDTO reviewEmpDetails(String empId) {
    Employee employee = employeeFacade.find(empId);
    if (employee != null) {
        EmployeeDTO empDTO = new EmployeeDTO(employee.getEmpid(),
                employee.getName(), employee.getPhone(), employee.getAddress(),
                employee.getEmail(), employee.getPassword(),
                employee.getAppGroup(), employee.getBnkAccId(),
                employee.getSalary(), employee.isActive());
        return empDTO;
    } else {
        return null;
    }

}
```

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

❖ index.xhtml

- homepage updated to let user have the option to log in as administrator or employee



```
<?xml version='1.0' encoding='UTF-8' ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"
      xmlns:h="http://java.sun.com/jsf/html">
    <head>
        <title>Secure Company's Home Page</title>
    </head>
    <body>

        <h1>
            Secure Company Ltd Home Page
        </h1>

        <h2>
            Welcome to our company
        </h2>

        <h3>
            We aim at developing secure enterprise application solutions to corporations.
        </h3>

        <h4>
            <a href="/ED-Secure-war/faces/admin/mainmenu.xhtml">
                1. Employee Management System (**Only for Admin**)
            </a>
        </h4>
        <h4>
            <a href="/ED-Secure-war/faces/user/mainmenu.xhtml">
                2. Employee Management System (For normal users, click here.)
            </a>
        </h4>

    </body>
</html>
```

❖ Newly added webpages for employee role

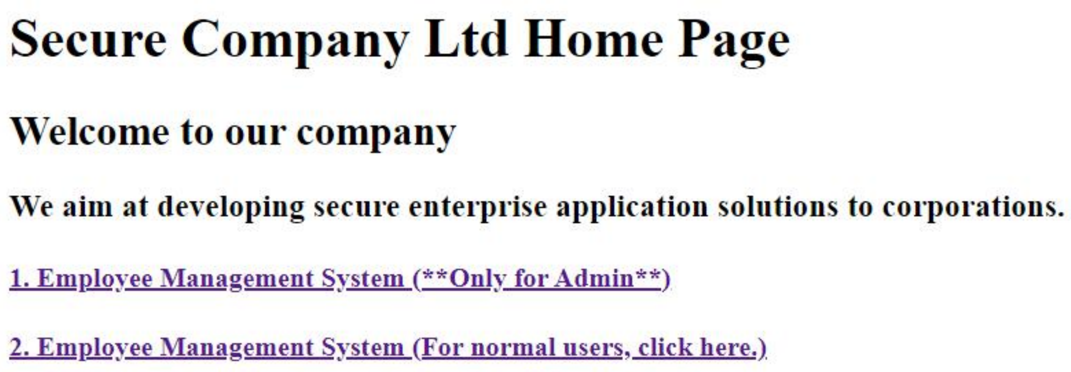
1. **mainmenu.xhtml**
2. **changeEmployee.xhtml**
3. **changeEmployeeDetails.xhtml**
4. **changeEmployeeSuccess.xhtml**
5. **changeEmployeeFailure.xhtml**
6. **changeEmployeeWrongPwd.xhtml**
7. **changePassword.xhtml**
8. **changePasswordSuccess.xhtml**
9. **changePasswordFailure.xhtml**
10. **displayEmployee.xhtml**
11. **displayEmployeeDetails.xhtml**
12. **displayEmployeeSuccess.xhtml**
13. **displayEmployeeFailure.xhtml**

This document is available free of charge on StuDocu.com

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

Task 7

1. Index.xhtml



Secure Company Ltd Home Page

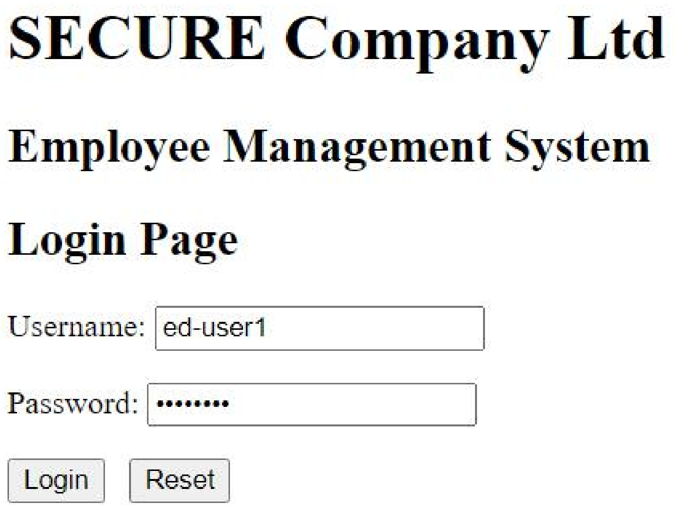
Welcome to our company

We aim at developing secure enterprise application solutions to corporations.

1. Employee Management System (Only for Admin**)**

2. Employee Management System (For normal users, click here.)

2. Index.xhtml



SECURE Company Ltd

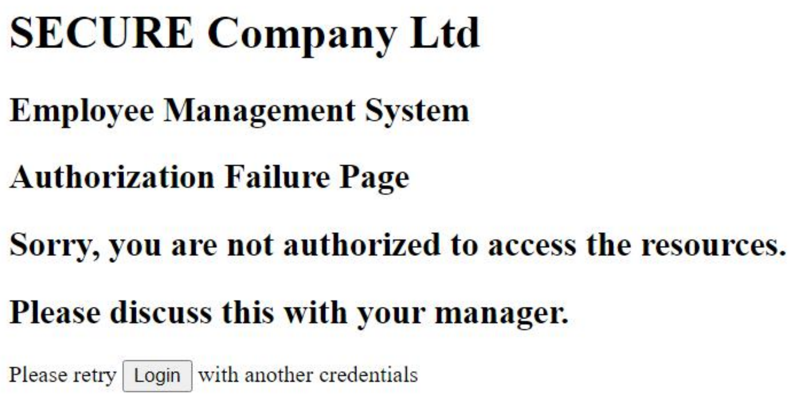
Employee Management System

Login Page

Username: ed-user1

Password: ••••••••

- Admin will not be able to access the employee page



SECURE Company Ltd

Employee Management System

Authorization Failure Page

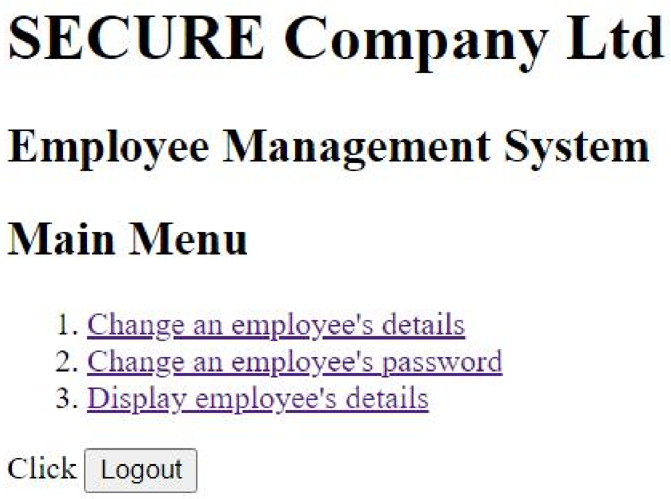
Sorry, you are not authorized to access the resources.

Please discuss this with your manager.

Please retry Login with another credentials

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

3. mainmenu.xhtml



SECURE Company Ltd

Employee Management System

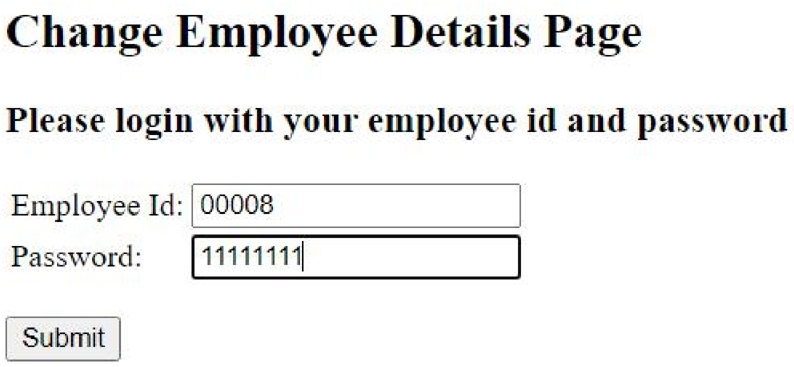
Main Menu

1. Change an employee's details
2. Change an employee's password
3. Display employee's details

Click

4. changeEmployee.xhtml

- Employee will need login using their id and password for changing the empployee details, to protect privacy.



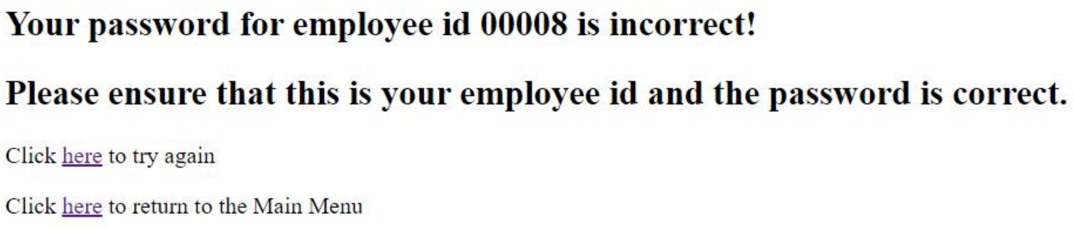
Change Employee Details Page

Please login with your employee id and password

Employee Id: 00008

Password: 11111111

- If password is incorrect, they will not be able to login



Your password for employee id 00008 is incorrect!

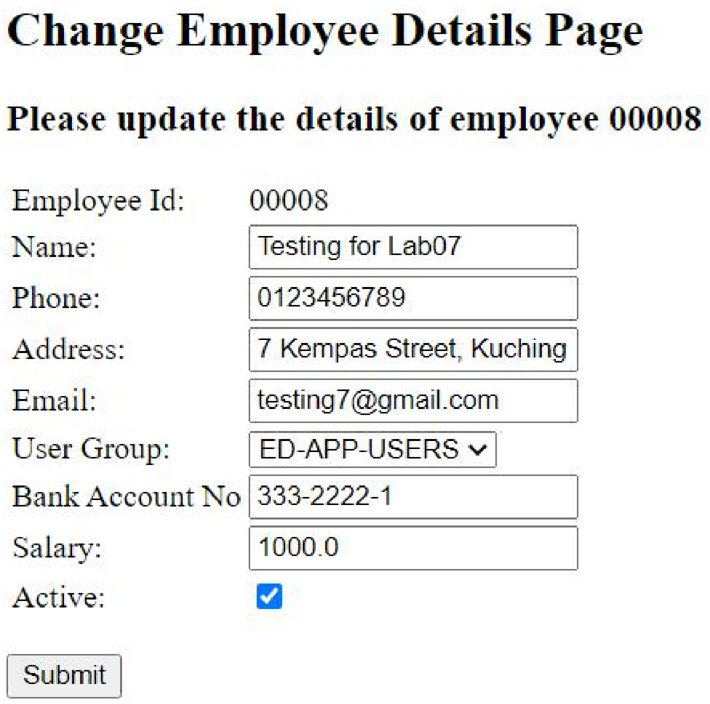
Please ensure that this is your employee id and the password is correct.

Click here to try again

Click here to return to the Main Menu

This document is available free of charge on StuDocu.com

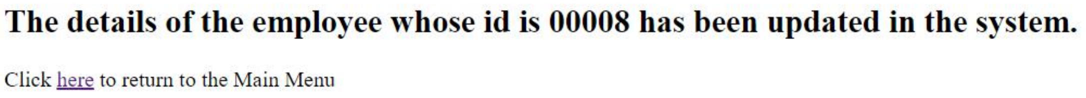
Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)



Change Employee Details Page

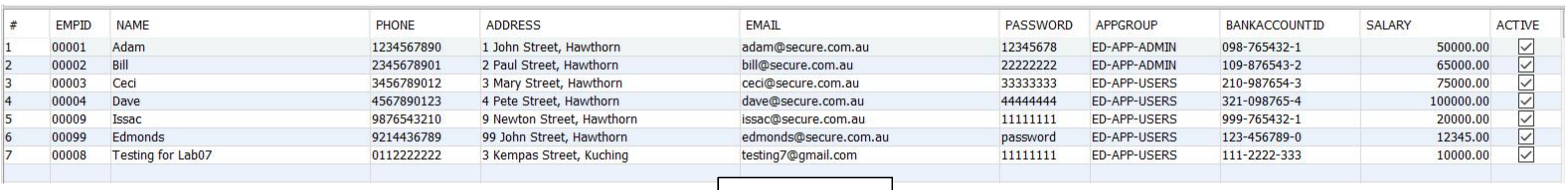
Please update the details of employee 00008

Employee Id:	00008
Name:	Testing for Lab07
Phone:	0123456789
Address:	7 Kempas Street, Kuching
Email:	testing7@gmail.com
User Group:	ED-APP-USERS
Bank Account No	333-2222-1
Salary:	1000.0
Active:	☑



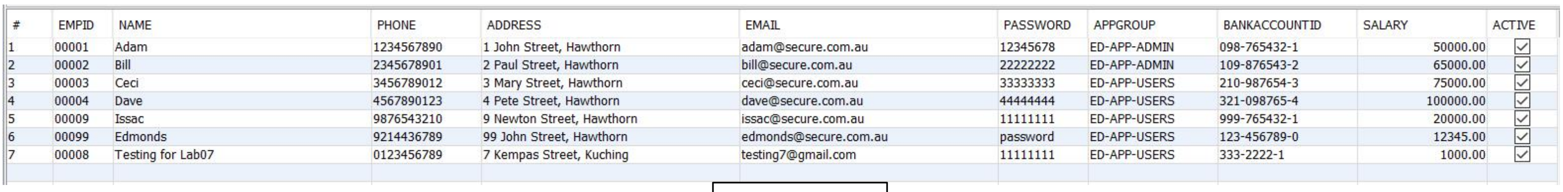
The details of the employee whose id is 00008 has been updated in the system.

Click here to return to the Main Menu



#	EMPID	NAME	PHONE	ADDRESS	EMAIL	PASSWORD	APPGROUP	BANKACCOUNTID	SALARY	ACTIVE
1	00001	Adam	1234567890	1 John Street, Hawthorn	adam@secure.com.au	12345678	ED-APP-ADMIN	098-765432-1	50000.00	☑
2	00002	Bill	2345678901	2 Paul Street, Hawthorn	bill@secure.com.au	22222222	ED-APP-ADMIN	109-876543-2	65000.00	☑
3	00003	Ceci	3456789012	3 Mary Street, Hawthorn	ceci@secure.com.au	33333333	ED-APP-USERS	210-987654-3	75000.00	☑
4	00004	Dave	4567890123	4 Pete Street, Hawthorn	dave@secure.com.au	44444444	ED-APP-USERS	321-098765-4	100000.00	☑
5	00009	Issac	9876543210	9 Newton Street, Hawthorn	issac@secure.com.au	11111111	ED-APP-USERS	999-765432-1	20000.00	☑
6	00099	Edmonds	9214436789	99 John Street, Hawthorn	edmonds@secure.com.au	password	ED-APP-USERS	123-456789-0	12345.00	☑
7	00008	Testing for Lab07	0112222222	3 Kempas Street, Kuching	testing7@gmail.com	11111111	ED-APP-USERS	111-2222-333	10000.00	☑

BEFORE



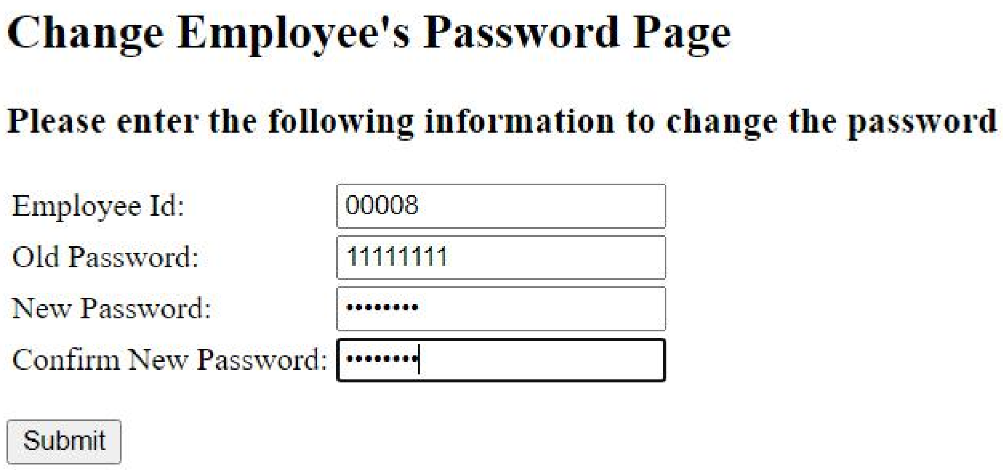
#	EMPID	NAME	PHONE	ADDRESS	EMAIL	PASSWORD	APPGROUP	BANKACCOUNTID	SALARY	ACTIVE
1	00001	Adam	1234567890	1 John Street, Hawthorn	adam@secure.com.au	12345678	ED-APP-ADMIN	098-765432-1	50000.00	☑
2	00002	Bill	2345678901	2 Paul Street, Hawthorn	bill@secure.com.au	22222222	ED-APP-ADMIN	109-876543-2	65000.00	☑
3	00003	Ceci	3456789012	3 Mary Street, Hawthorn	ceci@secure.com.au	33333333	ED-APP-USERS	210-987654-3	75000.00	☑
4	00004	Dave	4567890123	4 Pete Street, Hawthorn	dave@secure.com.au	44444444	ED-APP-USERS	321-098765-4	100000.00	☑
5	00009	Issac	9876543210	9 Newton Street, Hawthorn	issac@secure.com.au	11111111	ED-APP-USERS	999-765432-1	20000.00	☑
6	00099	Edmonds	9214436789	99 John Street, Hawthorn	edmonds@secure.com.au	password	ED-APP-USERS	123-456789-0	12345.00	☑
7	00008	Testing for Lab07	0123456789	7 Kempas Street, Kuching	testing7@gmail.com	11111111	ED-APP-USERS	333-2222-1	1000.00	☑

AFTER

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

5. changePassword.xhtml

- Employee will need enter the old password in order to change to a new one. This is to prevent others from changing your password without permission.

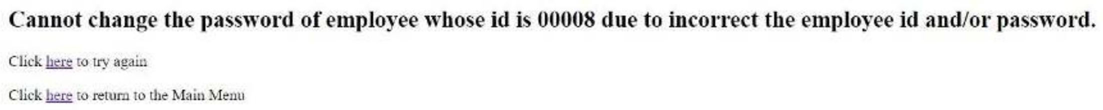


Change Employee's Password Page

Please enter the following information to change the password

Employee Id:	00008
Old Password:	11111111
New Password:	••••••••
Confirm New Password:	••••••••

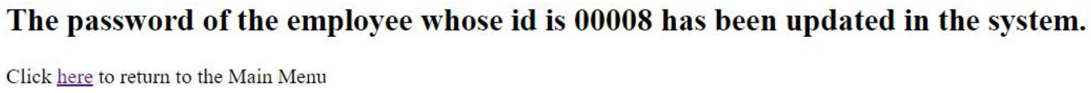
- If the password is wrong, password will not be changed.



Cannot change the password of employee whose id is 00008 due to incorrect the employee id and/or password.

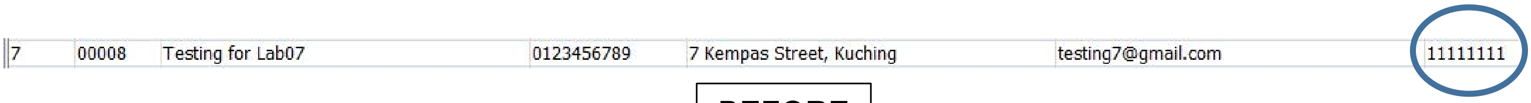
Click here to try again

Click here to return to the Main Menu



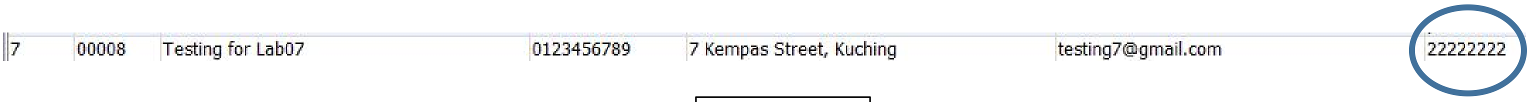
The password of the employee whose id is 00008 has been updated in the system.

Click here to return to the Main Menu



7	00008	Testing for Lab07	0123456789	7 Kempas Street, Kuching	testing7@gmail.com	11111111

BEFORE



7	00008	Testing for Lab07	0123456789	7 Kempas Street, Kuching	testing7@gmail.com	22222222

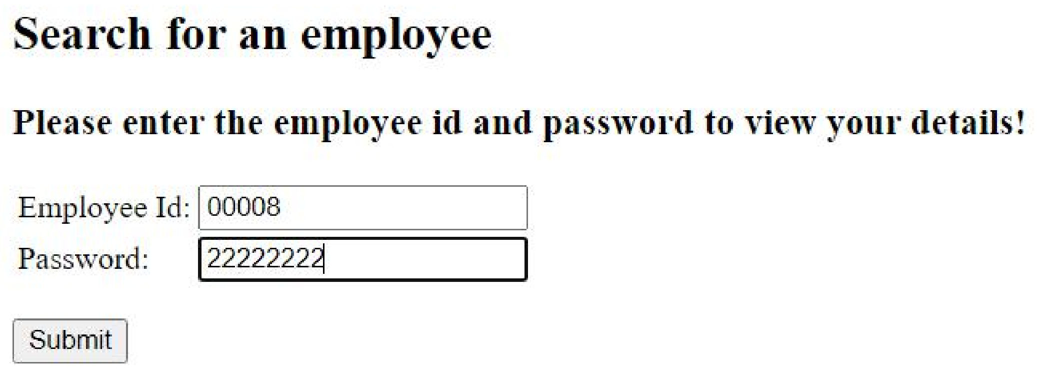
AFTER

This document is available free of charge on StuDocu.com

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)

6. displayEmployee.xhtml

- To display the employee details, user will also need to login, to keep the details private.

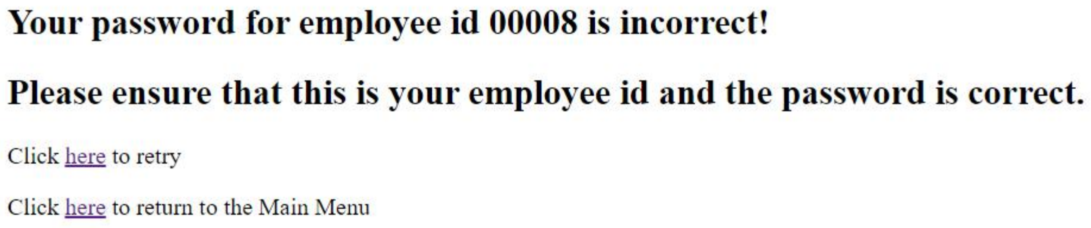


Search for an employee

Please enter the employee id and password to view your details!

Employee Id:	00008
Password:	22222222

- Wrong password will result in user not being able to display the employee details.

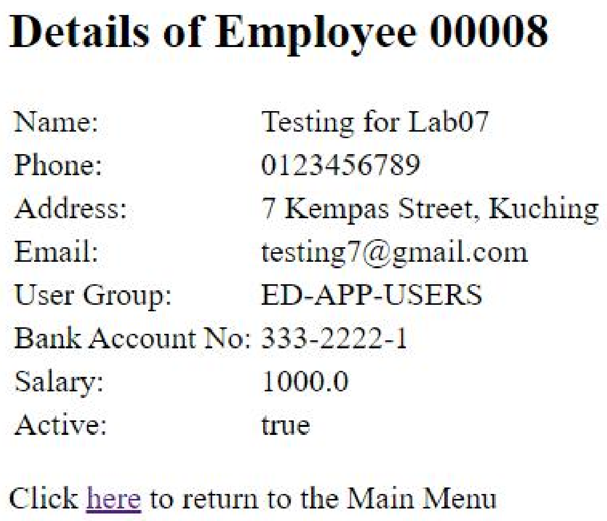


Your password for employee id 00008 is incorrect!

Please ensure that this is your employee id and the password is correct.

Click here to retry

Click here to return to the Main Menu



Details of Employee 00008

Name:	Testing for Lab07
Phone:	0123456789
Address:	7 Kempas Street, Kuching
Email:	testing7@gmail.com
User Group:	ED-APP-USERS
Bank Account No:	333-2222-1
Salary:	1000.0
Active:	true

Click here to return to the Main Menu

Downloaded by SM Ragib Rezwan (shaan66311@gmail.com)