Assignment-10

Name: Siddharth Sanskritayan

Roll No: 1901CS75

Task 1)

- MySQL is installed
- Xammp for Windows is installed using https://www.apachefriends.org/index.html (XAMPP is an Apache distribution containing MariaDB, PHP, and Perl.)

Task 2)

- Emp table is created using MySQL

```
mysql> create table emp(
    -> empID varchar(10) primary key,
    -> passwd varchar(255),
    -> empName varchar(20),
    -> DoJ date,
    -> salary int,
    -> department varchar(20),
    -> mobileNo int,
    -> email varchar(30));
Query OK, 0 rows affected (0.13 sec)
```
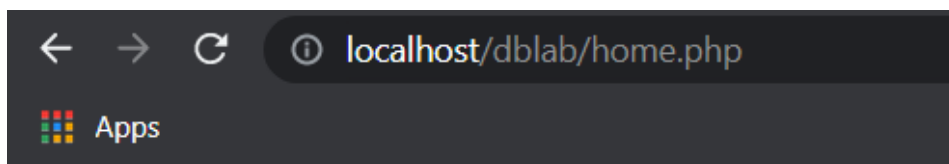
- Following pages are created:

- *home.php* :

```html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Home</title>
</head>
<body>
    <h2>Employee database</h2>
    <a href="registration.php">Register</a>
    <br>
    <a href="login.php">Login</a>
    <br>
    <a href="profileupdate.php">Update profile</a>
</body>
</html>
```

When opened in browser:

Employee database

Register
Login
Update profile

- *registration.php* :

```php
<?php include('server.php') ?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Registration</title>
</head>
<body>
    <div class="container">
        <h2>Register</h2>
        <form action="registration.php" method="post">
        <div>
            Employee ID <input type="text" name="empid" required><br>
        </div>
        <div>
            Password <input type="text" name="passwd" required><br>
        </div>
        <div>
            Employee Name <input type="text" name="empname" required><br>
        </div>
        <div>
            Date of Joining(YYYY-MM-DD) <input type="text" name="doj" required><br>
        </div>
        <div>
            Salary <input type="text" name="salary" required><br>
        </div>
        <div>
            Department <input type="text" name="department" required><br>
        </div>
        <div>
            Mobile No. <input type="text" name="mobileno" required><br>
        </div>
        <div>
            Email <input type="text" name="email" required><br>
        </div>
        <br>
        <button type="submit" name="register_user">Submit</button>
        </form>
        <br>
        <div><a href="home.php">Go to Home Page</a></div>
    </div>
</body>
</html>
```
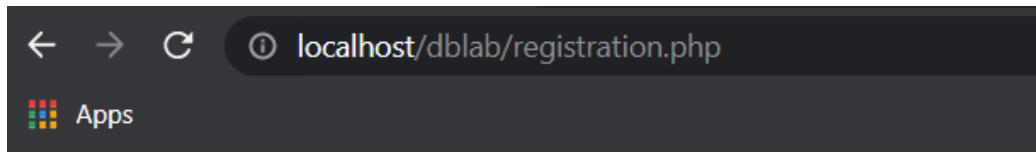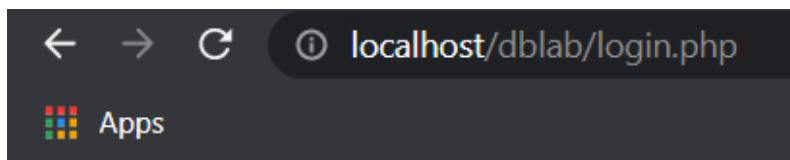
When opened in browser:

Register

Employee ID [   ]
Password [   ]
Employee Name [   ]
Date of Joining(YYYY-MM-DD) [   ]
Salary [   ]
Department [   ]
Mobile No. [   ]
Email [   ]

[Submit]

Go to Home Page

After inserting 5 records:


```
mysql> select * from emp;
+--------+--------------------------------------------------------------+----------+------------+---------+-------------+-----------+---------------------+
| empID  | passwd                                                       | empName  | DoJ        | salary  | department  | mobileNo  | email               |
+--------+--------------------------------------------------------------+----------+------------+---------+-------------+-----------+---------------------+
| E100   | $2y$10$3n/VMewIYFn7TP6ISOuPTe9fss97RgKViMIxy3Bf/vjiMegPOdeaa | rohan    | 2021-01-02 |   75000 | Testing     | 898698347 | rohan@gmail.com     |
| E101   | $2y$10$nE4xpfv9Nx7fLTiIka6QI.XNcp66ZSz0/BE632vJh6xhX16IjdYQq | Rohit    | 2021-03-06 |   80000 | IT services | 753583984 | rohit24@gmail.com   |
| E102   | $2y$10$YqNoFNyGiVo7A3GXkfBnTecE/ADJG0UX0ENlJS2TvtT5VkSynbU.G | Karan    | 2019-04-12 |  120000 | Sales       | 933476570 | karan@gmail.com     |
| E103   | $2y$10$S/pSKYoj089c0bDvXNNoleyt7BgA7y0SPP9mT8zWx/t/tOrdbVfI. | Mohit    | 2020-12-05 |   65000 | Marketing   | 764898591 | mohit01@yahoo.com   |
| E104   | $2y$10$C5fF0b47Ar0O0twSpqbmEeZaR0BU64Ybf0KfkdBJ4wsIlIqnuUI3y | Siddharth | 2021-02-03 | 1500000 | IT Services | 620484593 | sid@gmail.com       |
+--------+--------------------------------------------------------------+----------+------------+---------+-------------+-----------+---------------------+
5 rows in set (0.00 sec)
```

- *login.php* :

```php
<?php include('server.php') ?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Login</title>
</head>
<body>
    <div class="container">
        <h2>Login</h2>
        <form action="login.php" method="post">
        <div>
            Employee ID <input type="text" name="empid" required><br>
        </div>
        <div>
            Password <input type="text" name="passwd" required><br>
        </div>
        <button type="submit" name="login_user">Submit</button>
        </form>
        <br>
        <div><a href="home.php">Go to Home Page</a></div>
    </div>
</body>
</html>
```
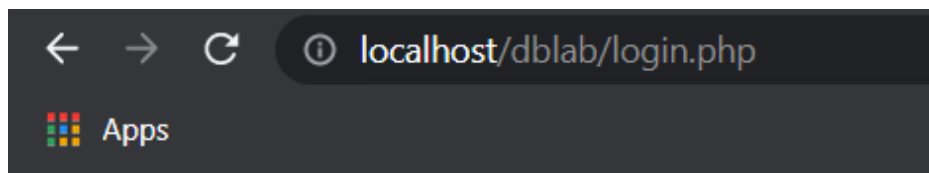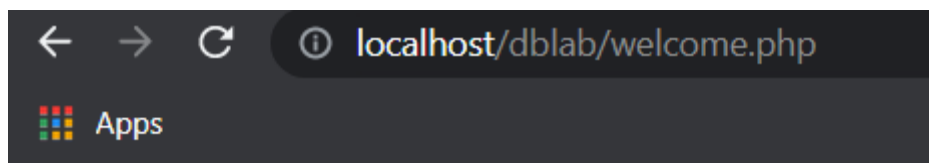
When opened in browser:

After logging in redirected to welcome.php

← → C ⓘ localhost/dblab/login.php

▦ Apps

Login

Employee ID E101
Password 101

Submit

Go to Home Page

← → C ⓘ localhost/dblab/welcome.php

▦ Apps

Logged in successfully

Welcome E101

Employee Name: Rohit
Date of Joining: 2021-03-06
Salary: 80000
Department: IT services
Mobile No.: 753583984
Email: rohit24@gmail.com
Logout

- *welcome.php* :

```php
<?php
session_start();

//User not logged in
if(!isset($_SESSION['empid']))
{
    echo "You need to login first <br>";
    header("location: login.php");
}

//if login is successfull
if(isset($_SESSION['success']))
{
    echo $_SESSION['success'];
    unset($_SESSION['success']);
}

//connecting to the database
$db=mysqli_connect('localhost','root','password','dblab');
if(!$db)
{
    echo "error connecting";
    die(mysql_error());
}
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Welcome</title>
</head>
<body>
    <div>
        <?php if(isset($_SESSION['empid'])): ?>
        <h3>Welcome <?php echo $_SESSION['empid'];?></h3>
        <?php
        $empid=$_SESSION['empid'];

        //fetching employee details
        $query="select * from emp where empid='$empid'";
```

```php
        $result=mysqli_query($db,$query);
        $user=mysqli_fetch_assoc($result);

        //Printing the employee details
        echo "Employee Name: " . $user['empName'] . "<br>";
        echo "Date of Joining: " . $user['DoJ'] . "<br>";
        echo "Salary: " . $user['salary'] . "<br>";
        echo "Department: " . $user['department'] . "<br>";
        echo "Mobile No.: " . $user['mobileNo'] . "<br>";
        echo "Email: " . $user['email'] . "<br>";

        ?>
        <a href="logout.php">Logout</a>
        <?php endif ?>

    </div>
</body>
</html>
```

Clicking Logout ends the session and redirects to home page

- *__logout.php__* :

```php
<?php
session_start();
$_SESSION=array();
session_destroy();
header("location: home.php");
?>
```

- *profileupdate.php* :

```php
<?php include('server.php') ?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>ProfileUpdate</title>
</head>
<body>
    <div class="container">
        <h2>Update Profile</h2>
        <form action="profileupdate.php" method="post">
        <div>
            Employee ID <input type="text" name="empid" required><br>
        </div>
        <div>
            Password <input type="text" name="passwd" required><br>
        </div>
        <div>
            Updated Mobile No. <input type="text" name="upmobileno" required><br>
        </div>
        <div>
            Updated Email <input type="text" name="upemail" required><br>
        </div>

        <button type="submit" name="update_user">Submit</button>
        </form>
        <br>
        <div><a href="home.php">Go to Home Page</a></div>
    </div>
</body>
</html>
```
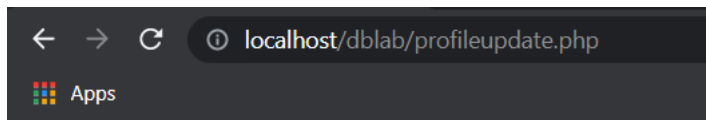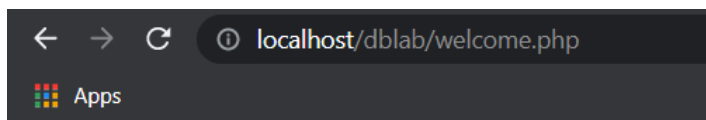
When opened in browser:

Update Profile

Employee ID E102
Password 102
Updated Mobile No. 967854000
Updated Email karan05@gmail.com
Submit

Go to Home Page

Upon successful update, we are redirected to welcome.php

Mobile no. and email updated successfully

Welcome E102

Employee Name: Karan
Date of Joining: 2019-04-12
Salary: 120000
Department: Sales
Mobile No.: 967854000
Email: karan05@gmail.com
Logout

Updated emp table after profile update:

```
mysql> select * from emp;
+-------+--------------------------------------------------------------+----------+------------+---------+-------------+----------+---------------------+
| empID | passwd                                                       | empName  | DoJ        | salary  | department  | mobileNo | email               |
+-------+--------------------------------------------------------------+----------+------------+---------+-------------+----------+---------------------+
| E100  | $2y$10$3n/VMewIYFn7TP6ISOuPTe9fss97RgKViMIxy3Bf/vjiMegPOdeaa | rohan    | 2021-01-02 |   75000 | Testing     | 898698347| rohan@gmail.com     |
| E101  | $2y$10$nE4xpfv9Nx7fLTiIka6QI.XNcp66ZSz0/BE632vJh6xhX16IjdYQq | Rohit    | 2021-03-06 |   80000 | IT services | 753583984| rohit24@gmail.com   |
| E102  | $2y$10$YqNoFNyGiVo7A3GXkfBnTecE/ADJG0UX0ENlJS2TvtT5VkSynbU.G | Karan    | 2019-04-12 |  120000 | Sales       | 967854000| karan05@gmail.com   |
| E103  | $2y$10$S/pSKYoj089c0bDvXNNoleyt7BgA7y0SPP9mT8zWx/t/tOrdbVfI. | Mohit    | 2020-12-05 |   65000 | Marketing   | 764898591| mohit01@yahoo.com   |
| E104  | $2y$10$C5fF0b47ArO0OtwSpqbmEeZaR0BU64Ybf0KfkdBJ4wsI1IqnuUI3y | Siddharth| 2021-02-03 | 1500000 | IT Services | 620484593| sid@gmail.com       |
+-------+--------------------------------------------------------------+----------+------------+---------+-------------+----------+---------------------+
5 rows in set (0.00 sec)
```

- *server.php* :

Backend for register.php, login.php and profileupdate.php

```php
<?php
session_start();
$errors=array();

//connecting to the database
$db=mysqli_connect('localhost','root','password','dblab');
if(!$db)
{
    echo "error connecting";
    die(mysql_error());
}


//if register submit button is clicked
if(isset($_POST['register_user']))
{
    $empid=mysqli_real_escape_string($db,$_POST['empid']);
    $passwd=mysqli_real_escape_string($db,$_POST['passwd']);
    $empname=mysqli_real_escape_string($db,$_POST['empname']);
    $doj=mysqli_real_escape_string($db,$_POST['doj']);
    $salary=mysqli_real_escape_string($db,$_POST['salary']);
    $department=mysqli_real_escape_string($db,$_POST['department']);
    $mobileno=mysqli_real_escape_string($db,$_POST['mobileno']);
    $email=mysqli_real_escape_string($db,$_POST['email']);

    // check emp table for existing employees with same empId or email
    $emp_check="select * from emp where empid='$empid' or email='$email' limit 1";
    $result=mysqli_query($db,$emp_check);
    $user=mysqli_fetch_assoc($result);

    if($user)
    {
        if($user['empID']===$empid)
        {
            array_push($errors,"EmpID already exists");
            echo "EmpID already exists" . "<br>";


        }
        if($user['email']===$email)
        {
            array_push($errors,"email already exists");
            echo "Email already exists";
```

```php
            }
        }


        //If no errors found
        if(count($errors)===0)
        {
            $hashedpasswd=password_hash($passwd,PASSWORD_DEFAULT);
            $query="Insert into emp values('$empid','$hashedpasswd','$empname','$doj','$salary','$departme
nt','$mobileno','$email')";
            mysqli_query($db,$query);


            $_SESSION['empid']=$empid;
            $_SESSION['success']="Registration Successful, you ar now logged in";
            //redirect to welcome page
            header('location: welcome.php');
        }
    }


//if login submit button is clicked
if(isset($_POST['login_user']))
{
    $empid=mysqli_real_escape_string($db,$_POST['empid']);
    $passwd=mysqli_real_escape_string($db,$_POST['passwd']);
    $query="select passwd from emp where empid='$empid'";
    $result=mysqli_query($db,$query);
    $user=mysqli_fetch_assoc($result);


    //check if password matches with the one stored in database
    if(password_verify($passwd,$user['passwd']))
    {
        $_SESSION['empid']=$empid;
        $_SESSION['success']="Logged in successfully";
        //redirect to welcome page
        header("location: welcome.php");
    }
    else
    {
        echo "Invalid Employee ID or password <br />";
    }


}


//if profile update submit button is clicked
if(isset($_POST['update_user']))
{
    $empid=mysqli_real_escape_string($db,$_POST['empid']);
    $passwd=mysqli_real_escape_string($db,$_POST['passwd']);
    $upmobileno=mysqli_real_escape_string($db,$_POST['upmobileno']);
```

```php
    $upemail=mysqli_real_escape_string($db,$_POST['upemail']);

    $query="select passwd from emp where empid='$empid'";
    $result=mysqli_query($db,$query);
    $user=mysqli_fetch_assoc($result);

    //check if password matches with the one stored in database
    if(password_verify($passwd,$user['passwd']))
    {
        $upquery1="update emp set mobileno='$upmobileno' where empID='$empid'";
        $upquery2="update emp set email='$upemail' where empID='$empid'";

        //update the emp table with the new values
        mysqli_query($db,$upquery1);
        mysqli_query($db,$upquery2);
        $_SESSION['empid']=$empid;
        $_SESSION['success']="Mobile no. and email updated successfully";

        //redirect to welcome page
        header("location: welcome.php");
    }
    else
    {
        echo "Invalid Employee ID or password <br />";
    }
}
?>
```