Kevin Davis
Cyber Security
11 March 2020

Deployment instructions

1. Unzip project folder and place the unzipped folder in your Eclipse workspace.
2. Import the database file (.sql file) into your default database (localhost port 3306)
3. Password for database should be "root" and the username should be "root"
4. Tomcat version 8.5 was used for the server (run on compatible server)
5. In Eclipse open index.html and run that page on server
6. You will be greeted with a login page, the user-names and passwords for the users, in the format (username|password), are as follows: (Alisha93|123456789) , (Amanda64|12345) , (kevin21|12345678) , (Raven96|1234) , (sugarlicious|12341) , (Troy59|6547239)

7. You can also create your own account by clicking ''Don't Have an Account ?''

Code and Explanation

XML file

```xml
<web-app>
version="3.0"
xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd" >

    <servlet>
        <servlet-name>register</servlet-name>
        <servlet-class>Register</servlet-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>register</servlet-name>
        <url-pattern>/register</url-pattern>
    </servlet-mapping>

    <servlet>
        <servlet-name>login</servlet-name>
        <servlet-class>Login</servlet-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>login</servlet-name>
        <url-pattern>/login</url-pattern>
    </servlet-mapping>

    <servlet>
        <servlet-name>logout</servlet-name>
        <servlet-class>Logout</servlet-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>logout</servlet-name>
        <url-pattern>/logout</url-pattern>
    </servlet-mapping>

    <servlet>
        <servlet-name>upload2</servlet-name>
        <servlet-class>Upload2</servlet-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>upload2</servlet-name>
        <url-pattern>/upload2</url-pattern>
    </servlet-mapping>

    <servlet>
        <servlet-name>welcome</servlet-name>
        <servlet-class>Welcome</servlet-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>welcome</servlet-name>
        <url-pattern>/welcome</url-pattern>
    </servlet-mapping>


    <welcome-file-list>
        <welcome-file>index.html</welcome-file>
    </welcome-file-list>
</web-app>
```

SignUp.html
This html page contains one form which takes all of the user data needed to create an account. When the
SignUp button is clicked, the information is sent to the Register servlet via the post method. This page uses
bootstrap for styling.

```html
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Student Data</title>
    <!-- Using bootstrap for design -->
    <link rel="stylesheet"
href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.1.3/css/bootstrap.min.css">
    <link rel="stylesheet"
href="https://cdnjs.cloudflare.com/ajax/libs/ionicons/2.0.1/css/ionicons.min.css">

<!-- ******************************* CSS ************************************** -->
<style>
.login-clean {
  background:#f1f7fc;
  padding:80px 0;
}
.login-clean form {
  max-width:320px;
  width:90%;
  margin:0 auto;
  background-color:#ffffff;
  padding:40px;
  border-radius:4px;
  color:#505e6c;
  box-shadow:1px 1px 5px rgba(0,0,0,0.1);
}
.login-clean .illustration {
  text-align:center;
  padding:0 0 20px;
  font-size:100px;
  color:rgb(244,71,107);
}
.login-clean form .form-control {
  background:#f7f9fc;
  border:none;
  border-bottom:1px solid #dfe7f1;
  border-radius:0;
  box-shadow:none;
  outline:none;
  color:inherit;
  text-indent:8px;
  height:42px;
}
.login-clean form .btn-primary {
  background:#f4476b;
  border:none;
  border-radius:4px;
  padding:11px;
  box-shadow:none;
  margin-top:26px;
  text-shadow:none;
  outline:none !important;
}
.login-clean form .btn-primary:hover, .login-clean form .btn-primary:active {
  background:#eb3b60;
}
.login-clean form .btn-primary:active {
```

```css
    transform:translateY(1px);
}
.login-clean form .forgot {
  display:block;
  text-align:center;
  font-size:12px;
  color:#6f7a85;
  opacity:0.9;
  text-decoration:none;
}
.login-clean form .forgot:hover, .login-clean form .forgot:active {
  opacity:1;
  text-decoration:none;
}
</style>

<!-- ****************************Register Form**************************************** -->
</head>
<body>
    <div class="login-clean">
    <!-- When the form is submitted it calls the register servlet -->
        <form method="post" action="register">
            <h2 class="sr-only">Login</h2>
            <div class="illustration"><i class="icon ion-ios-navigate"></i></div>
            <div class="form-group"><input class="form-control" type="text" name="username"
            placeholder="Username" required></div>
            <div class="form-group"><input class="form-control" type="password" name="pass"
            placeholder="Password" required></div>
            <div class="form-group"><input class="form-control" type="text" name="name"
            placeholder="Full name" required></div>
            <div class="form-group"><input class="form-control" type="text" name="field"
            placeholder="Field of Study" required></div>
            <div class="form-group"><input class="form-control" type="text" name="address"
            placeholder="Address" required></div>
            <div class="form-group"><input class="form-control" type="text" name="phone"
            placeholder="Phone Number" required></div>
            <div class="form-group"><input class="form-control" type="text" name="work"
            placeholder="Working Organization" required></div>
            <div class="form-group"><input class="form-control" type="text" name="title"
            placeholder="Job Title" required></div>
            <div class="form-group"><button class="btn btn-primary btn-block" name="register"
            type="submit">Sign Up</button></div>
            </form>
    </div>
</body>
</html>
```

Index.html
This html page contains one form which takes the username and password of a user. When the submit button is clicked the information is sent to the Login servlet via the post method. If the user does not have login credentials then they can click the sign up link to go to the sign up page. This page uses bootstrap for styling.

```html
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <title>Student Data</title>
        <!-- Using bootstrap for design -->
        <link rel="stylesheet"
href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.1.3/css/bootstrap.min.css">
        <link rel="stylesheet"
        href="https://cdnjs.cloudflare.com/ajax/libs/ionicons/2.0.1/css/ionicons.min.css">

    <!-- ******************************** CSS ******************************** -->
        <style>
        .login-clean
        {background:#f1f7fc;
          padding:80px 0;
        }
        .login-clean form
        { max-width:320px;
          width:90%;
          margin:0 auto;
          background-color:#ffffff;
          padding:40px;
          border-radius:4px;
          color:#505e6c;
          box-shadow:1px 1px 5px rgba(0,0,0,0.1);
        }
        .login-clean .illustration
        {text-align:center;
          padding:0 0 20px;
          font-size:100px;
          color:rgb(244,71,107);
          }
        .login-clean form .form-control
        {background:#f7f9fc;
          border:none;
          border-bottom:1px solid #dfe7f1;
          border-radius:0;
          box-shadow:none;
          outline:none;
          color:inherit;
          text-indent:8px;
          height:42px;
          }
        .login-clean form .btn-primary
        { background:#f4476b;
          border:none;
          border-radius:4px;
          padding:11px;
          box-shadow:none;
          margin-top:26px;
          text-shadow:none;
          outline:none !important;
          }
        .login-clean form .btn-primary:hover, .login-clean form .btn-primary:active
        { background:#eb3b60;
          }
        .login-clean form .btn-primary:active
```

```css
            {transform:translateY(1px);
            }
            .login-clean form .forgot
            {display:block;
              text-align:center;
              font-size:12px;
              color:#6f7a85;
              opacity:0.9;
              text-decoration:none;
              }
            .login-clean form .forgot:hover, .login-clean form .forgot:active
            {opacity:1;
              text-decoration:none;
              }
        </style>
    </head>

    <!-- ***************************Login Form********************************* -->
    <body>
    <!-- When the form is submitted it calls the login servlet -->
        <div class="login-clean">
            <form method="post" action="login">
                <h2 class="sr-only">Login</h2>
                <div class="illustration"><i class="icon ion-ios-navigate"></i></div>
                <div class="form-group"><input class="form-control" type="text" name="username"
                placeholder="Username" required></div>
                <div class="form-group"><input class="form-control" type="password" name="pass"
                placeholder="Password" required></div>
                <div class="form-group"><button class="btn btn-primary btn-block" name="Login"
                type="submit">Log In</button></div>
                <a href="SignUp.html" class="forgot">Don't Have an Account?</a></form>
        </div>
    </body>
</html>
```

Register Servlet

When this servlet is called it takes all the information from the form on the SignUp page and stores them into separate variables. It then connects to the database and stores the user name and password into the credentials table, and stores the other user data into the data table. If both tables are updated successfully the servlet will take the user to the Login page.

```java
import java.io.*;
import javax.servlet.*;
import javax.servlet.http.*;
import java.sql.*;
public class Register extends HttpServlet {
    protected void doPost(HttpServletRequest request, HttpServletResponse response)
        throws ServletException, IOException {
        response.setContentType("text/html;charset=UTF-8");
    //get data from form and store them
        String username = request.getParameter("username");
        String pass = request.getParameter("pass");
        String name = request.getParameter("name");
        String field = request.getParameter("field");
        String address = request.getParameter("address");
        String phone = request.getParameter("phone");
        String work = request.getParameter("work");
        String title = request.getParameter("title");
        try {
            // loading drivers for mysql
            Class.forName("com.mysql.jdbc.Driver");
            //creating connection with the database
            Connection con = DriverManager.getConnection
                ("jdbc:mysql://localhost:3306/students","root","root");
            //insert into username and password table
            PreparedStatement ps = con.prepareStatement("insert into credentials values(?,?)");
            ps.setString(1, username);
            ps.setString(2, pass);
            //insert into data table
            PreparedStatement py = con.prepareStatement
                ("insert into data(username,name,field_of_study,address,phone_number,"
                    + "working_organization,job_title) values(?,?,?,?,?,?,?)");
            py.setString(1, username);
            py.setString(2, name);
            py.setString(3, field);
            py.setString(4, address);
            py.setString(5, phone);
            py.setString(6, work);
            py.setString(7, title);
            int i = ps.executeUpdate();
            int j = py.executeUpdate();
            //if both tables have been updated successfully then go back to index
            if(i > 0 && j > 0)
                response.sendRedirect("index.html");
        }
        catch(Exception se) {se.printStackTrace();}
    }
}
```

Login Servlet

When this servlet is called it takes the information from the form on Login page and stores it into variables. After connecting to the database it checks the user name and password from the login page against the users in the database. If there is a match a session is started and the username and password is stored as session attributes. Then Welcome servlet is called. If either the username or password is incorrect, an incorrect username or password message is shown.

```java
import java.io.*;
import javax.servlet.*;
import javax.servlet.http.*;
import java.io.IOException;
import java.sql.*;
public class Login extends HttpServlet {
    protected void doPost(HttpServletRequest request, HttpServletResponse response)
        throws ServletException, IOException {
        response.setContentType("text/html;charset=UTF-8");
        //allows program to print to website
        PrintWriter out = response.getWriter();
        //get information from login form and store it in variables
        String username = request.getParameter("username");
        String pass = request.getParameter("pass");
        try { // loading drivers for mysql
            Class.forName("com.mysql.jdbc.Driver");
            //creating connection with the database
            Connection con = DriverManager.getConnection
                ("jdbc:mysql://localhost:3306/students","root","root");
            Statement stmt=con.createStatement();
            String sql="Select * from credentials where username "
                + "='"+username+"' and password = '"+pass+"'";
            ResultSet rs=stmt.executeQuery(sql);
            //if the Sql Statement has been executed correctly create
            //a session and call the welcome servlet
            if(rs.next()){
             HttpSession session = request.getSession();
              session.setAttribute("username", username);
              session.setAttribute("password", pass);
              //needs to work with request dispatcher for doPost
              RequestDispatcher requestDispatcher = request.getRequestDispatcher("welcome");
              requestDispatcher.forward(request, response);
            }else
            {    //if incorrect password or username
             out.println("Incorrect username or password....");
             out.println("<form action=\"index.html\" method=\"get\">");
             out.println("<input type=\"submit\" value=\"Try Again\" />");
            }
            con.close();
        }catch(Exception se) {se.printStackTrace();}
    }

}
```

Welcome Servlet
This servlet gets the username from the session attribute and selects all the user data related to that username and displays it on the web page. The web page is designed within the servlet for security reasons (so that users cannot access the page by url). The page is styled with bootstrap. To be consistant with the other pages, the same form layout was used. The user information is printed within the form tags. The user has the ability to use the form to upload a file. The file can be selected from any location on your local drive. There is also a description that can be added to the file. If there is no file allocated to that user the page will display "null" else it will display the description of the file. When the upload button is clicked the Upload servlet is called.

```java
import java.io.*;
import javax.servlet.*;
import javax.servlet.http.*;
import java.io.IOException;
import java.sql.*;
public class Welcome extends HttpServlet {
    protected void doPost(HttpServletRequest request, HttpServletResponse response)
        throws ServletException, IOException {
        response.setContentType("text/html;charset=UTF-8");
        //allows program to print to website
        PrintWriter out = response.getWriter();
        try {
        //get session information and store it in a variable
         HttpSession session = request.getSession();
            String username = (String) session.getAttribute("username");
          //connect to local database
            Class.forName("com.mysql.jdbc.Driver");
            Connection con = DriverManager.getConnection
                ("jdbc:mysql://localhost:3306/students","root","root");
            String sql2 = "SELECT * FROM data where username = '"+username+"' ";
            Statement stmt=con.createStatement();
            ResultSet data= stmt.executeQuery(sql2);

        //***************************Display Data on Webpage************************
        if (data.next()) {

            out.println("<html>");
            out.println("<head>");
            out.println("<meta charset=\"utf-8\">");
            out.println("<meta name=\"viewport\" content=\"width=device-width,"
                    + " initial-scale=1.0\">");
            out.println("<title>Student Data</title>");
            out.println(" <link rel=\"stylesheet\" href=\"https://cdnjs.cloudflare.com/ajax/libs/"
                    + "twitter-bootstrap/4.1.3/css/bootstrap.min.css\">");
            out.println("<link rel=\"stylesheet\" href=\"https://cdnjs.cloudflare.com/ajax/libs/"
                    + "ionicons/2.0.1/css/ionicons.min.css\">");

            //***********************************CSS***************************
            // Using bootstrap for design
            out.println("<style>");
            out.println(".login-clean \r\n" +
                    "          {\r\n" +
                    "             background:#f1f7fc;\r\n" +
                    "             padding:80px 0;\r\n" +
                    "          }");
            out.println(".login-clean form \r\n" +
                    "          {\r\n" +
                    "             max-width:320px;\r\n" +
                    "             width:90%;\r\n" +
                    "             margin:0 auto;\r\n" +
                    "             background-color:#ffffff;\r\n" +
                    "             padding:40px;\r\n" +
                    "             border-radius:4px;\r\n" +
```

```java
"            color:#505e6c;\r\n" +
"            box-shadow:1px 1px 5px rgba(0,0,0,0.1);\r\n" +
"        }");
out.println(".login-clean .illustration \r\n" +
"        {\r\n" +
"            text-align:center;\r\n" +
"            padding:0 0 20px;\r\n" +
"            font-size:100px;\r\n" +
"            color:rgb(244,71,107);\r\n" +
"        }");
out.println(".login-clean form .form-control \r\n" +
"        {\r\n" +
"            background:#f7f9fc;\r\n" +
"            border:none;\r\n" +
"            border-bottom:1px solid #dfe7f1;\r\n" +
"            border-radius:0;\r\n" +
"            box-shadow:none;\r\n" +
"            outline:none;\r\n" +
"            color:inherit;\r\n" +
"            text-indent:8px;\r\n" +
"            height:42px;\r\n" +
"        }");
out.println(".login-clean form .btn-primary \r\n" +
"        {\r\n" +
"            background:#f4476b;\r\n" +
"            border:none;\r\n" +
"            border-radius:4px;\r\n" +
"            padding:11px;\r\n" +
"            box-shadow:none;\r\n" +
"            margin-top:26px;\r\n" +
"            text-shadow:none;\r\n" +
"            outline:none !important;\r\n" +
"        }");
out.println(".login-clean form .btn-primary:hover, .login-clean form "
        + ".btn-primary:active \r\n" +
"        {\r\n" +
"            background:#eb3b60;\r\n" +
"        }");
out.println(".login-clean form .btn-primary:active \r\n" +
"        {\r\n" +
"            transform:translateY(1px);\r\n" +
"        }");
out.println(".login-clean form .forgot \r\n" +
"        {\r\n" +
"            display:block;\r\n" +
"            text-align:center;\r\n" +
"            font-size:12px;\r\n" +
"            color:#6f7a85;\r\n" +
"            opacity:0.9;\r\n" +
"            text-decoration:none;\r\n" +
"        }");
out.println(".login-clean form .forgot:hover, .login-clean form "
        + ".forgot:active \r\n" +
"        {\r\n" +
"            opacity:1;\r\n" +
"            text-decoration:none;\r\n" +
"        }");
out.println("</style>");
out.println("</head>");
out.println("<body>");

//********************User Information Printed**************************

out.println("<div class=\"login-clean\">");
//logout form
out.println("<form action=\"logout\" method=\"post\">");
out.println("<input type=\"submit\" value=\"Logout\" />");
```

```java
            out.println("</form>");
            //beginning of form that contains all data on this page
            //this form will call the upload2 servlet
            out.println("<form method=\"post\" action=\"upload2\" "
                    + "enctype=\"multipart/form-data\">");
            out.println("<div class=\"illustration\"><i "
                    + "class=\"icon ion-ios-navigate\"></i></div>");
            out.println("<div class=\"form-group\"> <b>Name: </b>"
                    + data.getString("name") + "</div>");
            out.println("<div class=\"form-group\"> <b>Field of Study: </b>"
                    + data.getString("field_of_study") + "</div>");
            out.println("<div class=\"form-group\"> <b>Address: </b>"
                    + data.getString("address") + "</div>");
            out.println("<div class=\"form-group\"> <b>Phone Number: </b>"
                    + data.getString("phone_number") + "</div>");
            out.println("<div class=\"form-group\"> <b>Working Organization: </b>"
                    + data.getString("working_organization") + "</div>");
            out.println("<div class=\"form-group\"> <b>Job Title: </b>"
                    + data.getString("job_title") + "</div>");

            //****************************Select file ************************************
            out.println("<div class=\"form-group\">");
            //file input
            out.println("<input type=\"file\" name =\"file\" class=\"form-control-file\">");
            out.println("</div>");
            //description input
            out.println("<div class=\"form-group\"><input class=\"form-control\" "
                    + "type=\"text\" name=\"description\" placeholder=\"File Description\"></div>");
            out.println("<div class=\"form-group\"><button class=\"btn btn-primary btn-block\" "
                    + "name=\"upload\" type=\"Upload\">Upload File</button></div>");

            //*************************** Shows if a file is stored***************************
            out.println("<b>File Stored: </b>");
            try {
                Statement data_stmt=con.createStatement();
                ResultSet data_rs = data_stmt.executeQuery("SELECT * "
                        + "FROM data where username = '"+username+"' ");
                //if there is a file, print the description
                if(data_rs.next()) {out.println(data_rs.getString(9));}
                else {out.println("None");}
            }
            catch(Exception p){System.out.println(p);}
            //end of form and rest of page
            out.println("</form>");
            out.println("</div> ");
            out.println("</body>");
            out.println("</html>");
        }
        con.close();
        }
        catch(Exception se) {
            se.printStackTrace();
        }
    }
}
```

Upload2
```java
import java.io.IOException;
import java.io.InputStream;
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import javax.servlet.*;
import javax.servlet.annotation.MultipartConfig;
import javax.servlet.http.*;
@MultipartConfig()
public class Upload2 extends HttpServlet {
    protected void doPost(HttpServletRequest request, HttpServletResponse response)
        throws ServletException, IOException{
    response.setContentType("text/html;charset=UTF-8");
        try{
        //get session information and store in a variable
            HttpSession session = request.getSession();
            String username = (String) session.getAttribute("username");
            //get data from form and store them
            String description = request.getParameter("description");
            //connect to local database
        String url = "jdbc:mysql://localhost:3306/students";
            String user = "root";
            String password = "root";
            Connection conn = DriverManager.getConnection(url, user, password);
            // input stream of the upload file
            InputStream inputStream = null;
            // obtains the upload file part in this multipart request
            Part filePart = request.getPart("file");
            inputStream = filePart.getInputStream();
            //update the file and file description cells with new values
            String sql = "UPDATE data SET file = (?), file_description = "
                + "(?) WHERE username = '"+username+"' ";
            PreparedStatement statement = conn.prepareStatement(sql);
            statement.setBlob(1, inputStream);
            statement.setString(2, description);
            int row = statement.executeUpdate();
            //if atleast 1 row is returned from the execution, then it was a success
            if (row > 0)
            conn.close();
            //response.sendRedirect("welcome");

            //needs to work with request dispatcher for doPost
            RequestDispatcher requestDispatcher = request.getRequestDispatcher("welcome");
             requestDispatcher.forward(request, response);
         }
        catch(Exception se) { se.printStackTrace(); }
    }
}
```

Logout Servlet

```java
import java.io.IOException;
import javax.servlet.*;
import javax.servlet.http.*;

public class Logout extends HttpServlet
{
    @Override
    protected void doPost(HttpServletRequest request, HttpServletResponse response)
        throws ServletException, IOException {
    HttpSession session = request.getSession();
    //destroy session
    session.invalidate();
        response.sendRedirect("index.html");
    }
}
```

The Database
The database contains 2 tables.

The first table is named "credentials" and it contains 2 columns. The first column is username and the other is password. Username is the primary key of the table.

The second table is named "data" contains 9 columns; username, name, field_of_study, address, phone_number, working_organization, job_title, file and file_description.