

# ***LOG IN & REGISTRATION PAGE PROJECT***

**COMP 440 Project phase 1**

- SAMUEL SARKISIAN
- SHIVA RAMEZANI
- CESAR BARRERA

# Code: signup.php

- for handling unmatched passwords and duplicate cases that fall under username, email, and/or both
- Handles empty user input, which will ask the user to fill in the slot

```
if(!empty($username) && !empty($password) && !empty($passwordconfirmed)&& !empty($firstName) && !empty($lastName) && !empty($email)){
    if ($password != $passwordconfirmed){
        echo("password and passwordconfirmed does not match, please try again");
    }
    else{
        $sql = "INSERT INTO user (username,password,firstName,lastName,email) VALUES (?, ?, ?, ?, ?)";
        $stmt = mysqli_stmt_init($con);

        if(!mysqli_stmt_prepare($stmt, $sql)){
            echo("issue...");
        }
        else{
            $q_username = "SELECT username FROM user WHERE username = '$username' ";
            $result_username = mysqli_query($con,$q_username);
            $num_rows_username = mysqli_num_rows($result_username);

            $q_email = "SELECT email FROM user WHERE email = '$email'";
            $result_email = mysqli_query($con,$q_email);
            $num_rows_email = mysqli_num_rows($result_email);
            // check for duplicates in database
            if(!$num_rows_username && !$num_rows_email)
            {
                //save to database
                mysqli_stmt_bind_param($stmt, "sssss", $username, $password, $firstName, $lastName, $email);
                mysqli_stmt_execute($stmt);
                header("Location: login.php");
                exit;
            }
            elseif($num_rows_username && $num_rows_email)
            {
                echo" Duplicate email and username please try again";
            }
            elseif($num_rows_username)
            {
                echo" Duplicate username please try again";
            }
            elseif($num_rows_email)
            {
                echo" Duplicate email please try again";
            }
        }
    }
}
else
{
    echo "Empty slot for user input, please fill in";
}
```

# GUI: Sign Up Page

- This is a visualization of the sign up page that our application outputs



Signup

username:

password:

password confirmed:

first name:

last name:

email:

[Signup](#)

[Click to Login](#)

# Code: signup.php

- errors for duplicate username, email, or both

```
if(!$num_rows_username && !$num_rows_email)
{
    //save to database

    mysqli_stmt_bind_param($stmt, "sssss", $username, $password, $firstName, $lastName, $email);
    mysqli_stmt_execute($stmt);
    header("Location: login.php");
    die;
}

elseif($num_rows_username && $num_rows_email)
{
    echo "Duplicate email and username please try again";
}

elseif($num_rows_username)
{
    echo "Duplicate username please try again";
}

elseif($num_rows_email)
{
    echo "Duplicate email please try again";
}
```

# GUI: Signup Page Duplication Errors

Duplicate email and username please try again

Signup

username:

Duplicate username please try again

Signup

username:

Duplicate email please try again

Signup

username:

# GUI: Sign Up Error for empty user input

Empty slot for user input, please fill in

## Signup

username:

password:

password confirmed:

first name:


last name:

email:

Signup

[Click to Login](#)

# After successfully signing up



The screenshot displays a database management interface. On the left, a sidebar shows a tree view of databases and tables. The 'comp440\_project' database is selected, and the 'user' table is highlighted. The main area shows the SQL editor with the following query:

```
SELECT * FROM `user`
```

Below the query, there are buttons for 'Profiling', 'Edit inline', 'Edit', 'Explain SQL', 'Create PHP code', and 'Refresh'. The 'Edit inline' button is active.

The SQL editor also shows the following query:

```
UPDATE `user` SET `email` = 'JohnSmith@gmail.com' WHERE `user`.`username` = 'John';
```

Below the queries, there are buttons for 'Edit inline', 'Edit', and 'Create PHP code'. The 'Edit inline' button is active.

Below the buttons, there are controls for 'Show all', 'Number of rows' (set to 25), 'Filter rows' (Search this table), and 'Sort by key' (None).

Below the controls, there is a '+ Options' button and a table view showing the contents of the 'user' table. The table has columns: 'username', 'password', 'firstName', 'lastName', and 'email'. The table contains one row with the following data:

username	password	firstName	lastName	email
John	122*efw	John	Smith	JohnSmith@gmail.com

# Code: login.php

- Handles empty user input, which will ask the user to fill in the slot and takes checks user

```
session_start();

include("connection.php");
include("operations.php");
//var_dump($_SERVER);
$requestMethod = strtoupper(getenv('REQUEST_METHOD'));
$httpMethods = array('GET', 'POST', 'PUT', 'DELETE', 'HEAD', 'OPTIONS');

if (in_array($requestMethod, $httpMethods))
{
    if ($requestMethod == 'POST') {

        $username = $_POST['username'];
        $password = $_POST['password'];
        $firstName = $_POST['firstName'];
        $lastName = $_POST['lastName'];
        $email = $_POST['email'];

        if(!empty($username) && !empty($password) && !empty($firstName) && !empty($lastName) && !empty($email) && !is_numeric($username))
        {
            $query = "select * from user where username = '$username' limit 1";
            $result = mysqli_query($con, $query);

            if($result)
            {
                if($result && mysqli_num_rows($result) > 0)
                {
                    $user_data = mysqli_fetch_assoc($result);

                    if(($user_data['password'] === $password) && ($user_data['firstName'] === $firstName) && ($user_data['lastName'] === $lastName) && ($user_data['email'] === $email))
                    {
                        $_SESSION['username'] = $user_data['username'];
                        header("Location: index.php");
                        exit;
                    }
                }
            }

            echo "incorrect credentials!";
        }
        else
        {
            echo "Empty slot for user input, please fill it in!";
        }
    }
}
else{
    echo("failed server");
}
```



# GUI: Login page



Login

username:

password:

first name:

last name:

email:

Login

[Click to Signup](#)

- This is a visualization of the login page that our application outputs

# GUI: Login Error for Empty User Input

Empty slot for user input, please fill it in!

## Login

username:

password:

first name:


last name:

email:

Login

[Click to Signup](#)

## GUI: Login page Logging in with incorrect credentials



incorrect credentials!

Login

username:

password:

The image shows a web application interface with a light pink background. On the left, a white rectangular area contains the text 'incorrect credentials!' in a dark grey font. To the right of this is a green rectangular area. Inside the green area, the word 'Login' is written in a blue, serif font. Below 'Login', the text 'username:' is followed by a white text input field with rounded ends. Below the input field, the text 'password:' is followed by a white password input field with rounded ends and a small eye icon on the right side.

# Code: index.php

```
<?php
session_start();

    include("connection.php");
    include("operations.php");

    $user_data = check_login($con);

?>

<!DOCTYPE html>
<html>
<head>
    <title>My website</title>
</head>
<body>

    <a href="logout.php">Logout</a>
    <h1>This is the index page</h1>

    <br>
    Hello, <?php echo $user_data['username']; ?>

    <br></br>

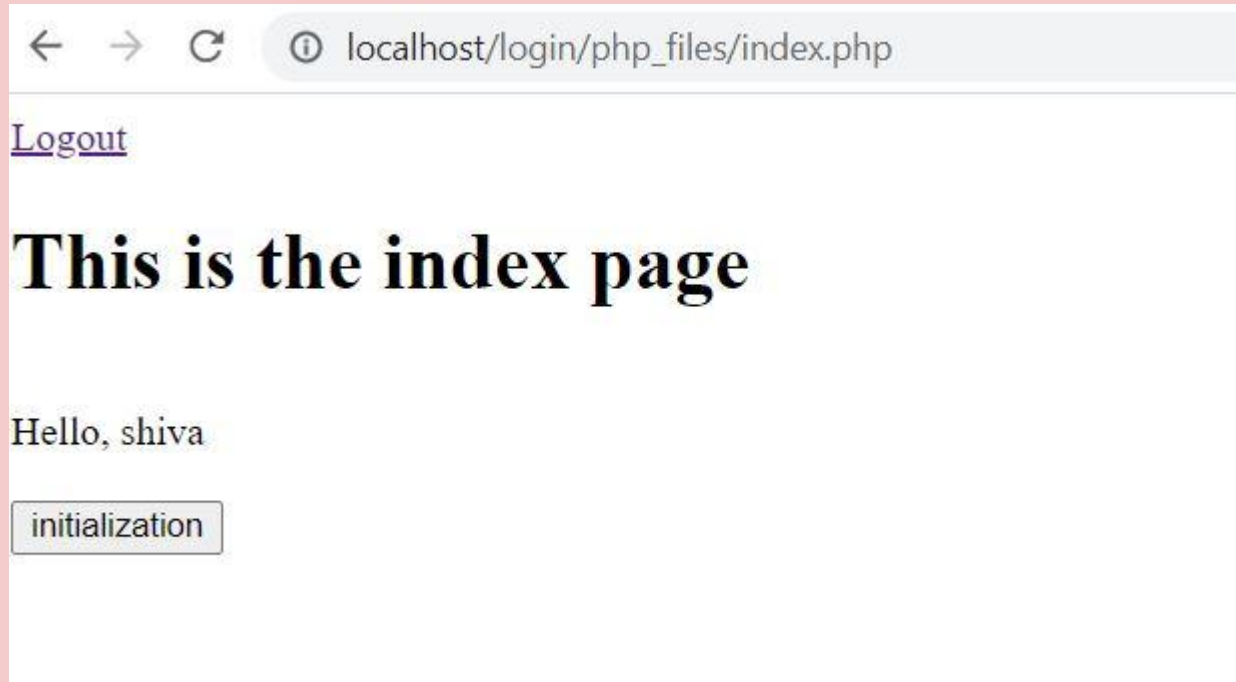
    <input type="button" value="initialization" onclick="location='initialize_database.php'" />

</body>
</html>
```

- After the user logs in they will encounter the website where we have a welcome message with a logout and initialize database functionality

# GUI: Index page

- This is a visualization of the website after user logs in, which our application outputs



## Code: logout.php

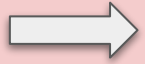
- Unsets session username, which is our primary id

```
!k?php
session_start();

if(isset($_SESSION['username']))
{
    unset($_SESSION['username']);
}

header("Location: login.php");
exit;
```

GUI: logout



[Logout](#)

**This is the index page**

## Code : Initializing\_database.php && project.sql

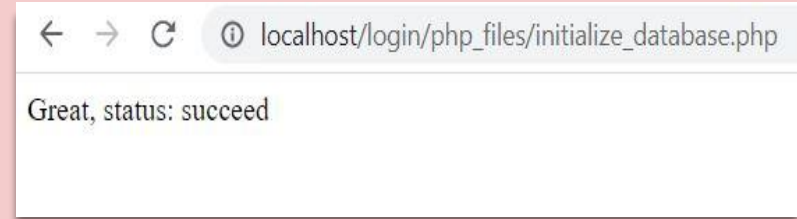
```
<?php
$mysql_host = "localhost";
$mysql_database = "comp440_project";
$mysql_user = "comp440";
$mysql_password = "pass1234";
$db = new PDO("mysql:host=$mysql_host; dbname=$mysql_database", $mysql_user, $mysql_password);
$query = file_get_contents("project.sql");
$stmt = $db->prepare($query);

if ($stmt->execute()){
    echo "Great, status: succeed";
}
else{
    echo "Issue, status: failed";
}
```

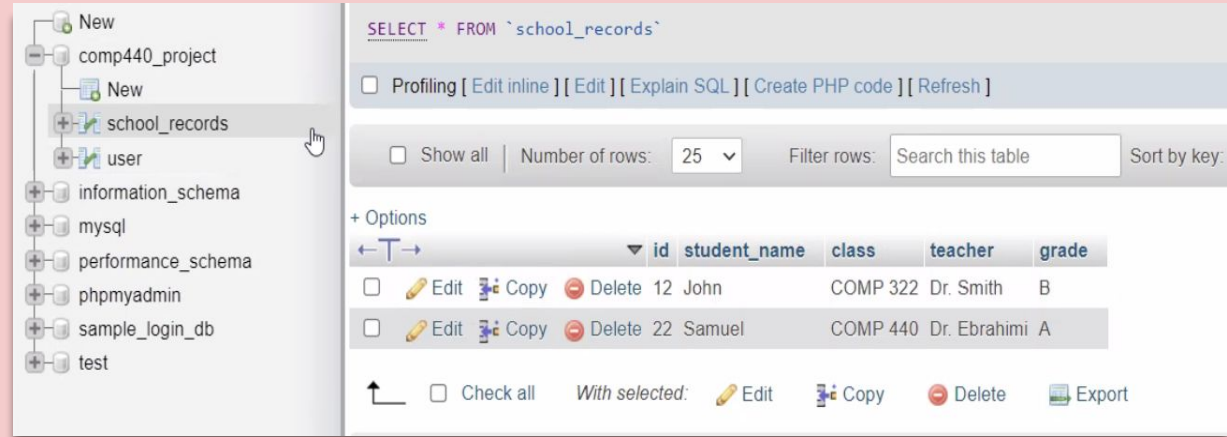
```
DROP TABLE IF EXISTS `school_records`;
create table school_records (id INT, student_name varchar(20), class varchar(45), teacher varchar(45), grade varchar(100), primary key (id) );
INSERT INTO `school_records` VALUES (12,'John','COMP 322','Dr. Smith','B'),(22,'Samuel','COMP 440','Dr. Ebrahimi','A');
```



# Initialization successful



- Initializes table called school\_records, which drops the table if it exists and populates the table with the information shown here



# signup.php: SQL Injection Prevention

```
//input user given info for registration while preventing sql injection
$username = mysqli_real_escape_string($con, $_POST['username']);
$password = mysqli_real_escape_string($con,$_POST['password']);
$firstName = mysqli_real_escape_string($con,$_POST['firstName']);
$lastName = mysqli_real_escape_string($con,$_POST['lastName']);
$email = mysqli_real_escape_string($con,$_POST['email']);
$passwordconfirmed = mysqli_real_escape_string($con,$_POST['passwordconfirmed']);
```

```
// check for duplicates in database
if(!$num_rows_username && !$num_rows_email)
{
    //save to database
    mysqli_stmt_bind_param($stmt, "sssss", $username, $password, $firstName, $lastName, $email);
    mysqli_stmt_execute($stmt);
    header("Location: login.php");
    exit;
}
```

```
else{
    $sql = "INSERT INTO user (username,password,firstName,lastName,email) VALUES (?, ?, ?, ?, ?)";
    $stmt = mysqli_stmt_init($con);

    if(!mysqli_stmt_prepare($stmt, $sql)){
        echo("issue...");
    }
}
```

## Code: operations.php

- Check to see if an individual is Logged In

```
function check_login($con)
{
    if(isset($_SESSION['username']))
    {
        $username = $_SESSION['username'];
        $query = "select * from user where username = '$username' limit 1";

        $result = mysqli_query($con,$query);
        if($result && mysqli_num_rows($result) > 0)
        {
            $user_data = mysqli_fetch_assoc($result);
            return $user_data;
        }
    }

    header("Location: login.php");
    exit;
}
```

## Code: connection.php

- Connects the application to the database without root privileges

```
k?php

$dbhost = "localhost";
$dbuser = "comp440";
$dbpass = "pass1234";
$dbname = "comp440_project";

if(!$con = mysqli_connect($dbhost,$dbuser,$dbpass,$dbname))
{
    echo("failed to connect!");
    exit();
}
```