LOG IN & REGISTRATION PROJECT

COMP 440 Project Phase 1

Geek Squad

Team # 14

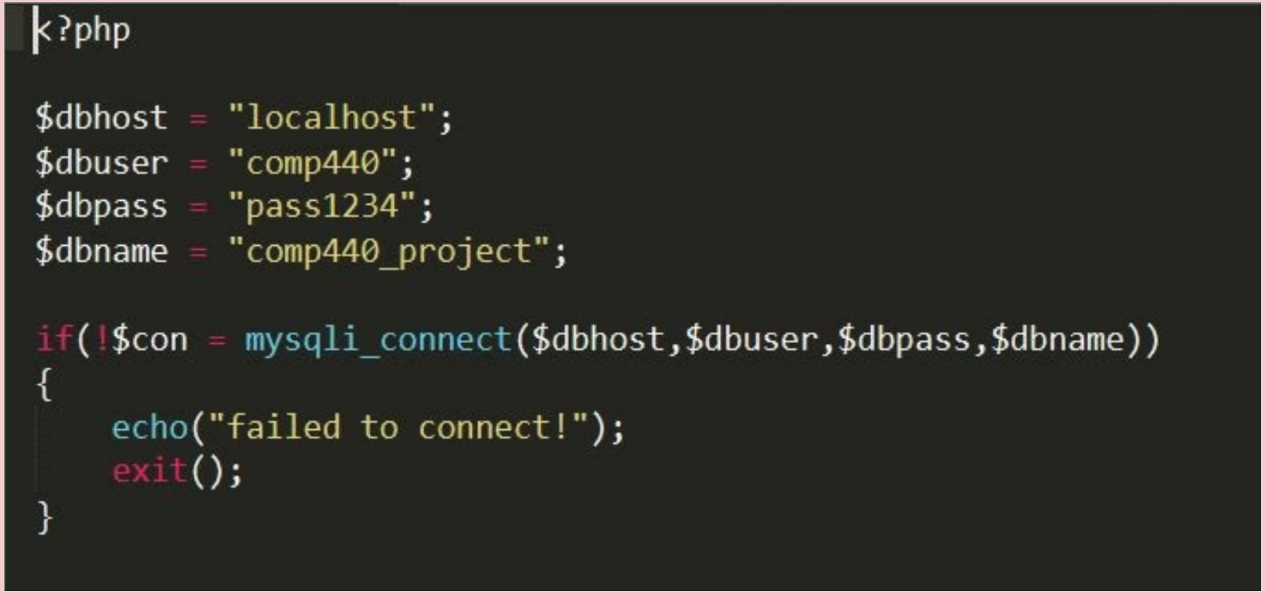
- SAMUEL SARKISIAN
- SHIVA RAMEZANI
- CESAR BARRERA

Files

- connection.php
- signup.php
- Login.php
- operations.php
- index.php
- logout.php
- initilize_database.php
- project.sql

Code: connection.php

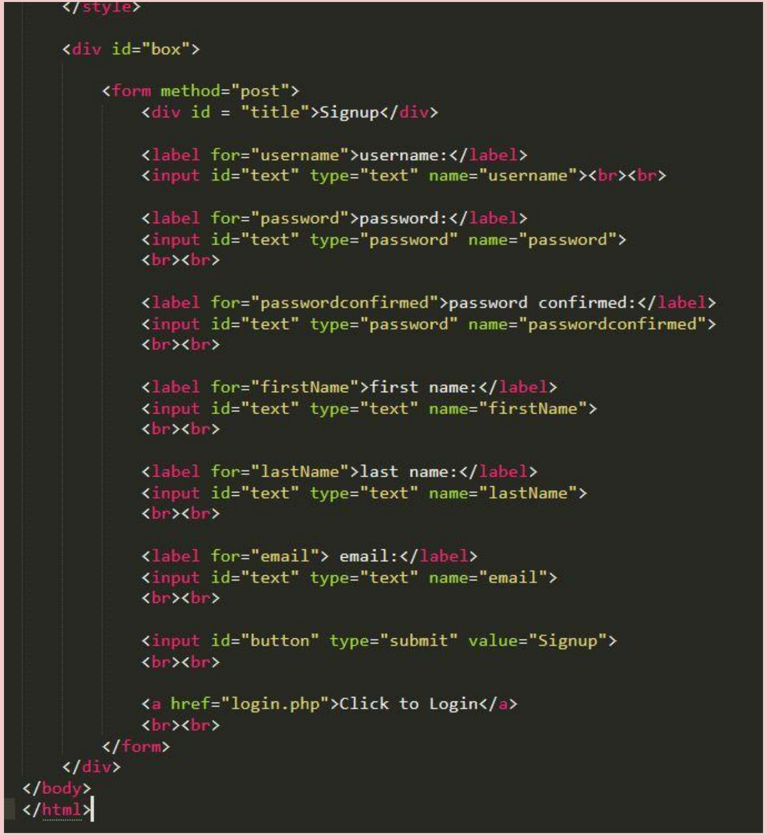
- Connects the application to the database without root privileges



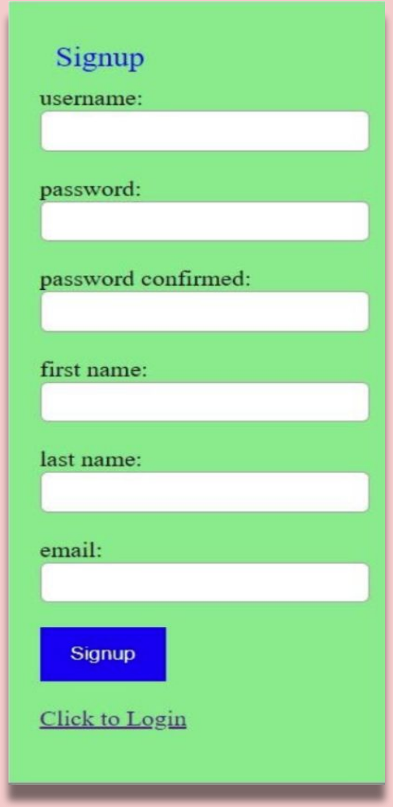
```php
<?php

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

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

GUI: Sign Up Page

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

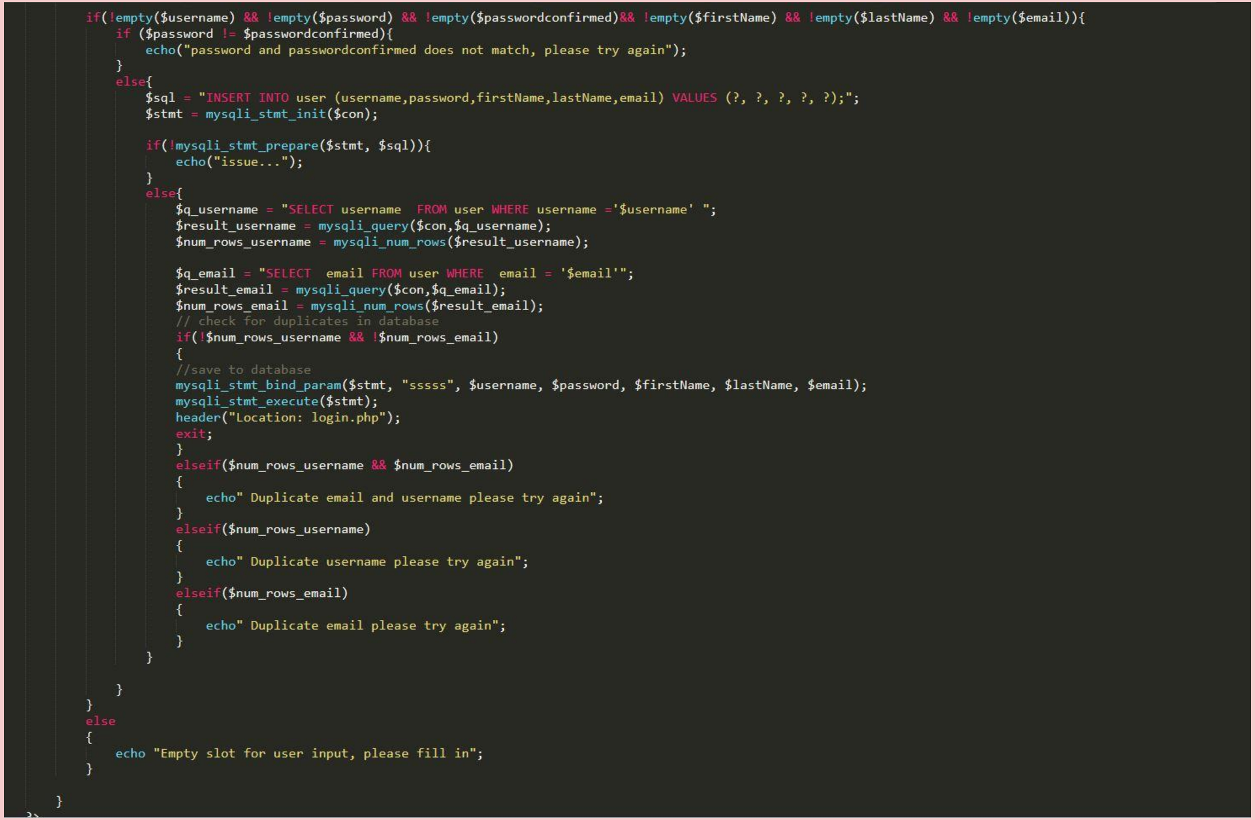


```
    </style>

    <div id="box">

        <form method="post">
            <div id = "title">Signup</div>

            <label for="username">username:</label>
            <input id="text" type="text" name="username"><br><br>

            <label for="password">password:</label>
            <input id="text" type="password" name="password">
            <br><br>

            <label for="passwordconfirmed">password confirmed:</label>
            <input id="text" type="password" name="passwordconfirmed">
            <br><br>

            <label for="firstName">first name:</label>
            <input id="text" type="text" name="firstName">
            <br><br>

            <label for="lastName">last name:</label>
            <input id="text" type="text" name="lastName">
            <br><br>

            <label for="email"> email:</label>
            <input id="text" type="text" name="email">
            <br><br>

            <input id="button" type="submit" value="Signup">
            <br><br>

            <a href="login.php">Click to Login</a>
            <br><br>
        </form>
    </div>
</body>
</html>
```



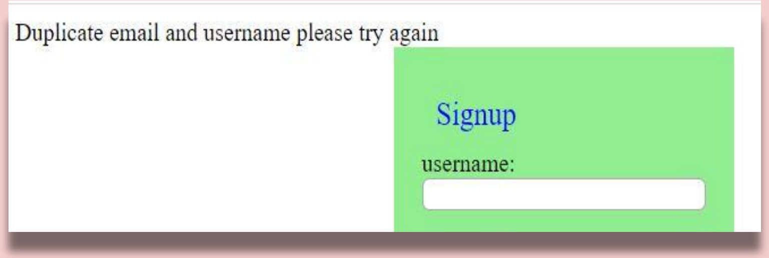
Code: signup.php

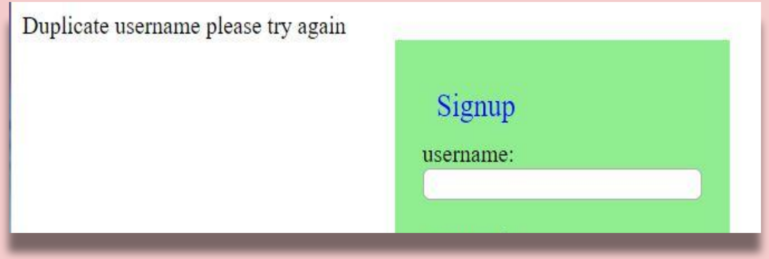
- for handling unmatched passwords and duplicate cases that fall under username, email, and/or both
- Handles empty user input, which will ask the user to fill in the slot

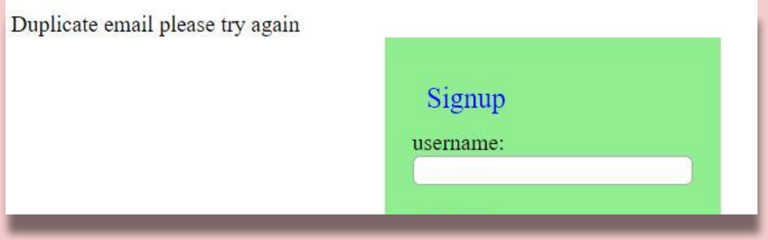


```
        if(!empty($username) && !empty($password) && !empty($passwordconfirmed)&& !empty($firstName) && !empty($lastName) && !empty($email)){
            if ($password != $passwordconfirmed){
                echo("password and passwordconfirmed does not match, please try again");
            }
            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";
        }

    }
?>
```

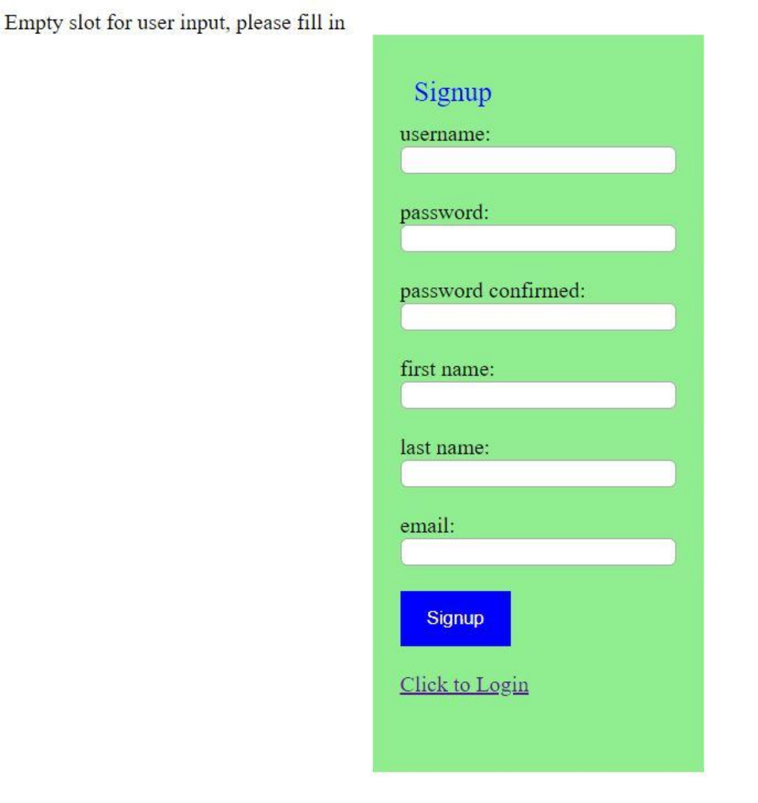
GUI: Signup Page Duplication Errors


Duplicate email and username please try again


Duplicate username please try again


Duplicate email please try again

GUI: Sign Up Error for empty user input



Empty slot for user input, please fill in

Signup

username:

password:

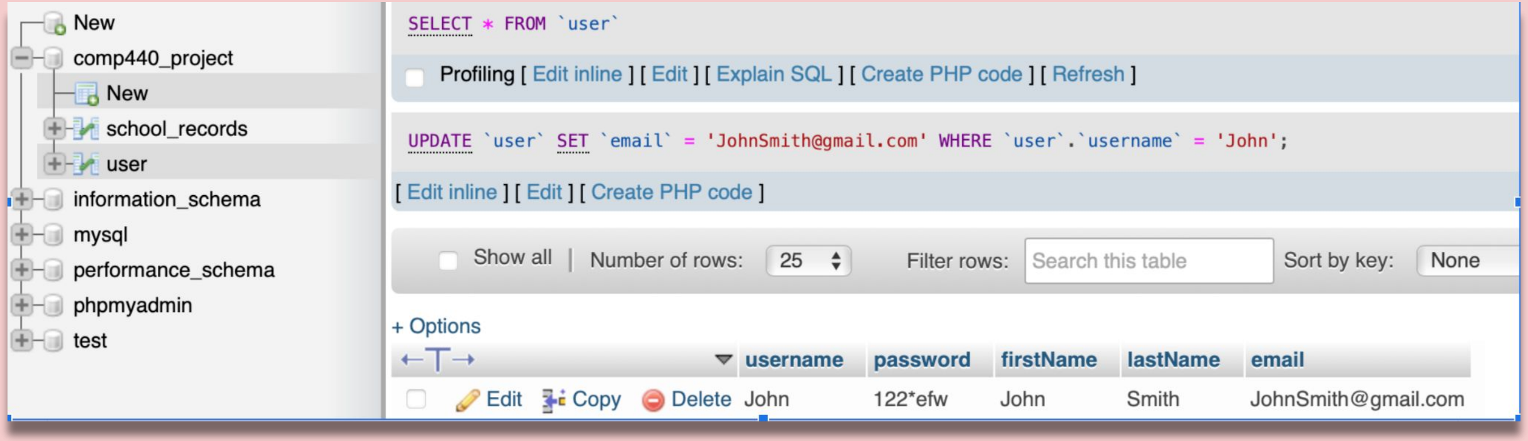
password confirmed:

first name:

last name:

email:

After successfully signing up



New
comp440_project
New
school_records
user
information_schema
mysql
performance_schema
phpmyadmin
test

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

Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

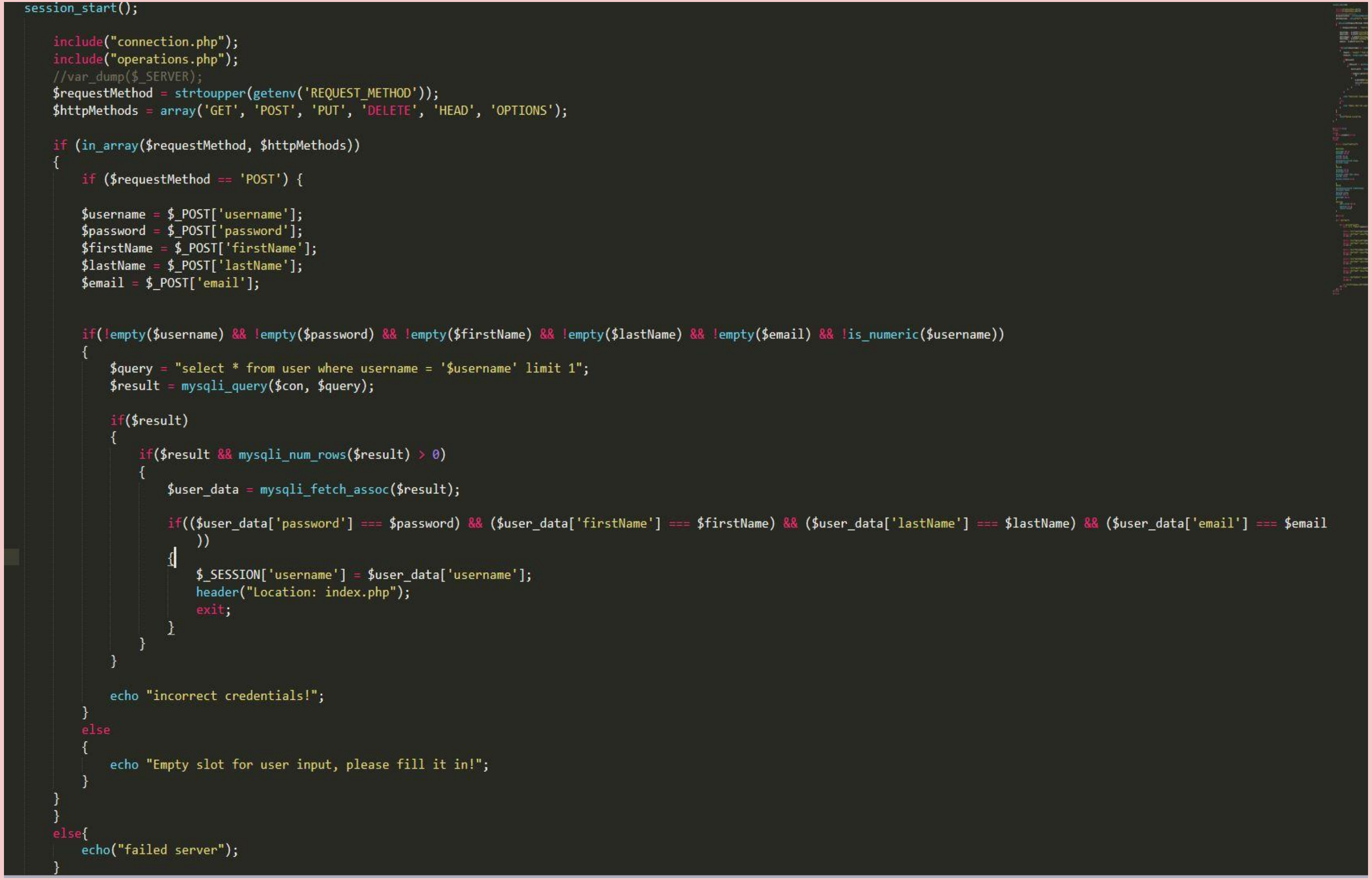
```
UPDATE `user` SET `email` = 'JohnSmith@gmail.com' WHERE `user`.`username` = 'John';
```

[Edit inline] [Edit] [Create PHP code]
Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None
+ Options

	username	password	firstName	lastName	email
□ Edit Copy Delete	John	122*efw	John	Smith	JohnSmith@gmail.com

Code: login.php

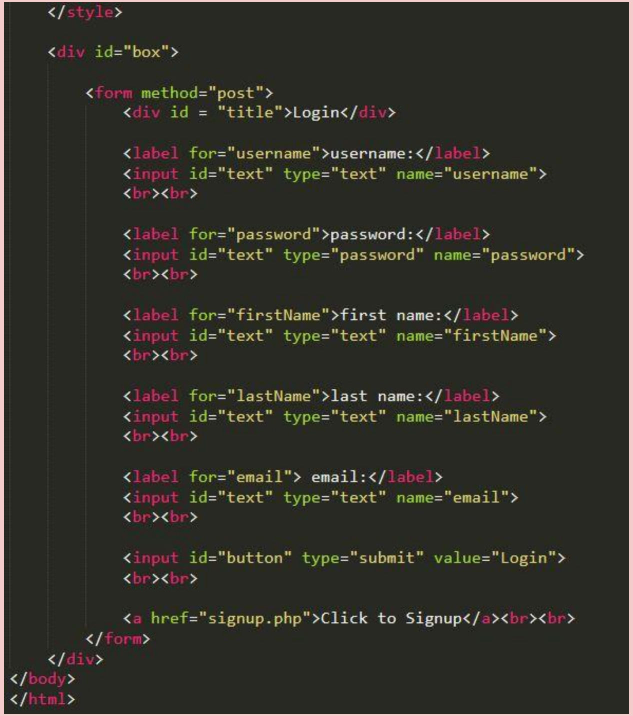
- Asks the user to fill in the slots and checks the user’s credentials according to our database to see if they match. Also, it handles empty user input. If all is satisfactory then it will grant access



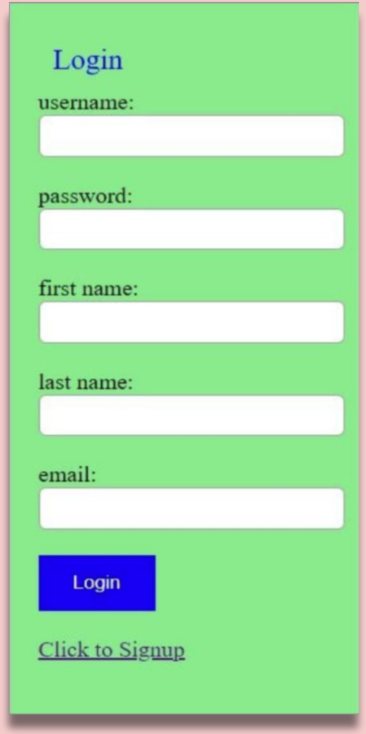
```
session_start();

    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

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



```
    </style>

    <div id="box">

        <form method="post">
            <div id = "title">Login</div>

            <label for="username">username:</label>
            <input id="text" type="text" name="username">
            <br><br>

            <label for="password">password:</label>
            <input id="text" type="password" name="password">
            <br><br>

            <label for="firstName">first name:</label>
            <input id="text" type="text" name="firstName">
            <br><br>

            <label for="lastName">last name:</label>
            <input id="text" type="text" name="lastName">
            <br><br>

            <label for="email"> email:</label>
            <input id="text" type="text" name="email">
            <br><br>

            <input id="button" type="submit" value="Login">
            <br><br>

            <a href="signup.php">Click to Signup</a><br><br>
        </form>
    </div>
</body>
</html>
```



Login

username:

password:

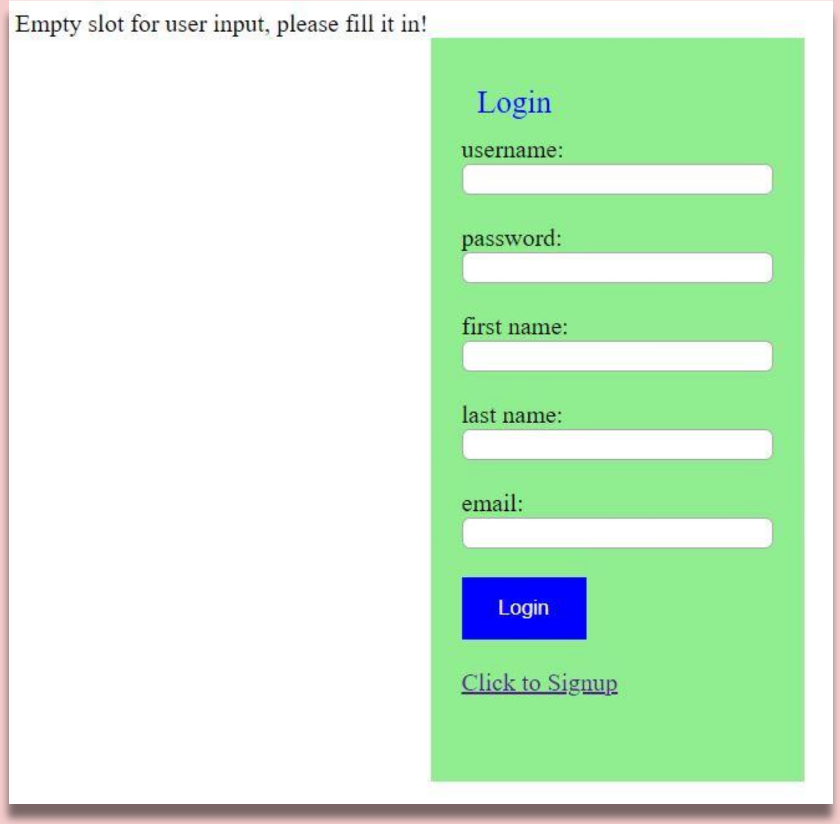
first name:

last name:

email:

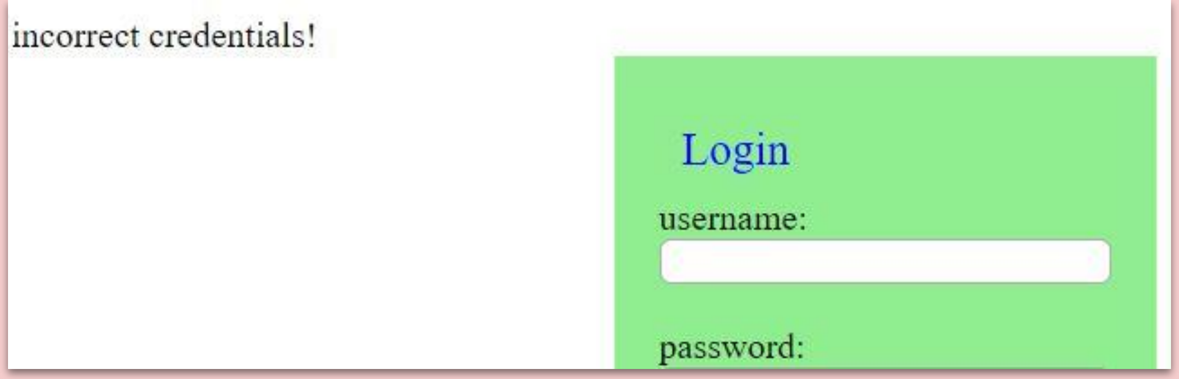
Click to Signup

GUI: Login Error for Empty User Input



Empty slot for user input, please fill it in!

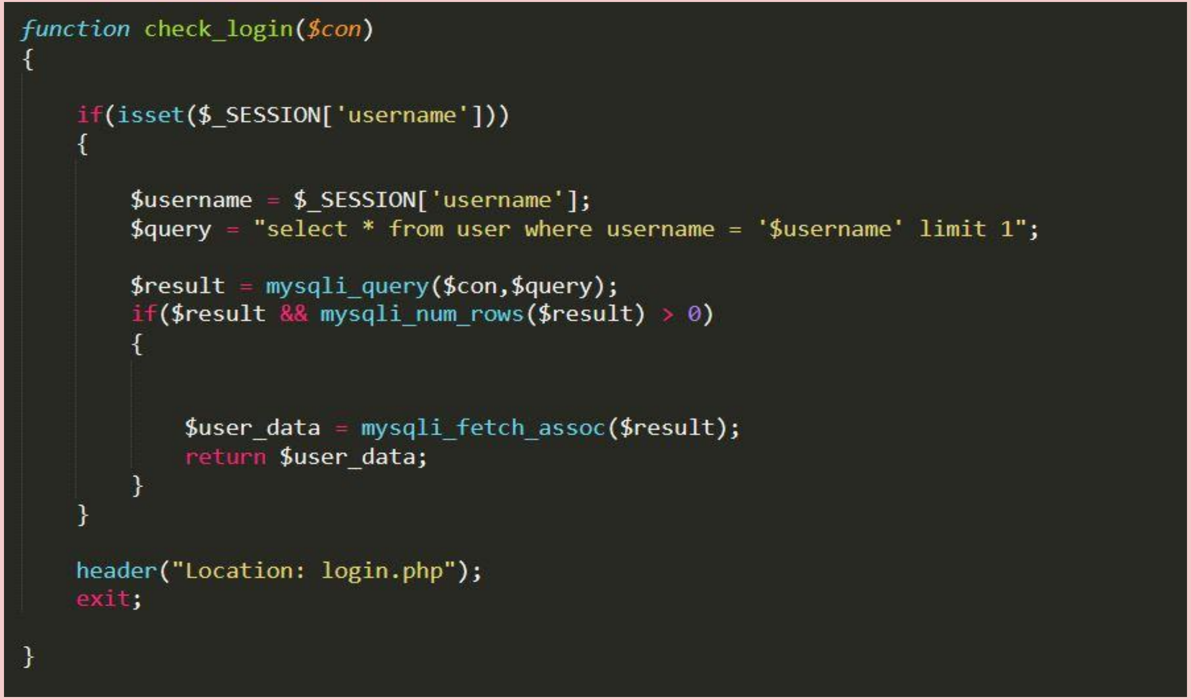
GUI: Login page Logging in with incorrect credentials



incorrect credentials!

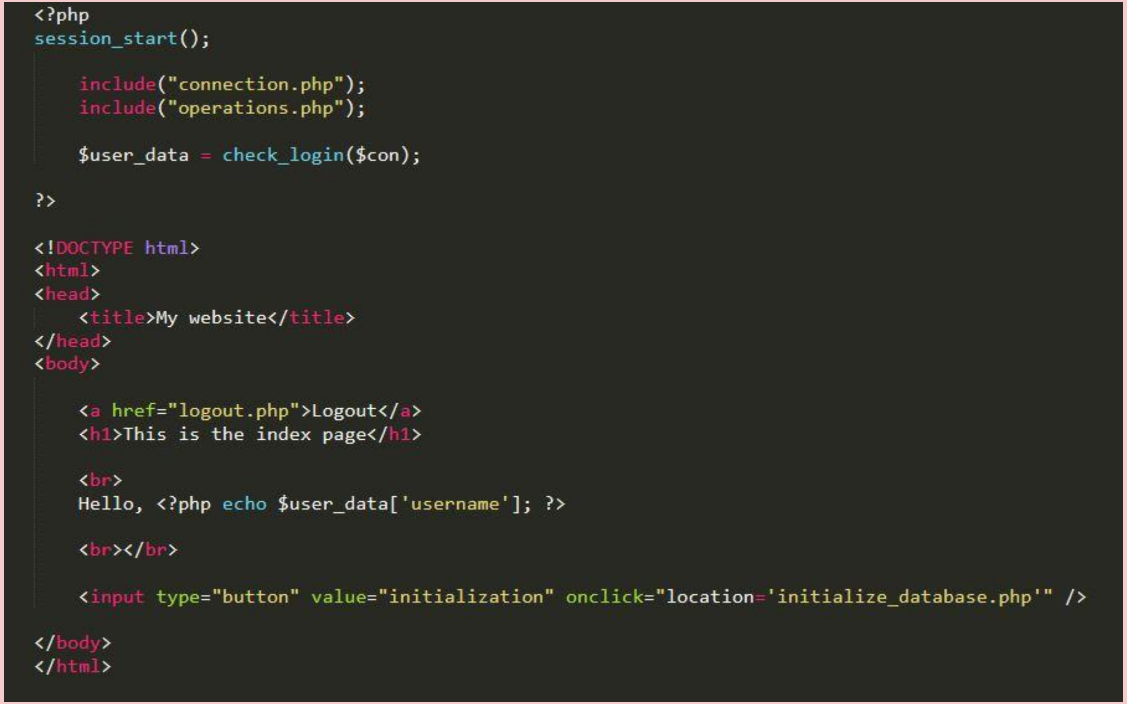
Code: operations.php

- Check to see if an individual is Logged In



```php
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: index.php

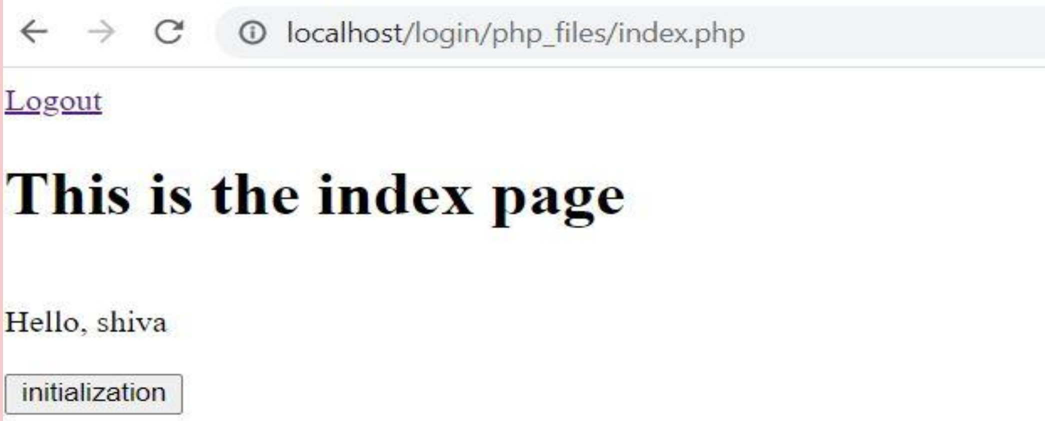


```
<?php
session_start();

    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

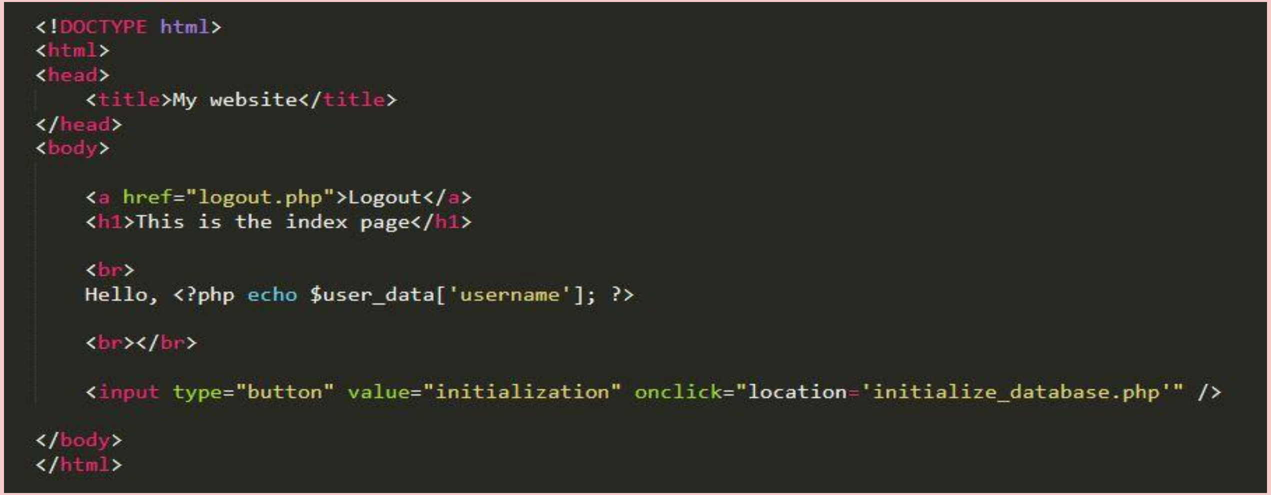
GUI: Index page

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



This is the index page

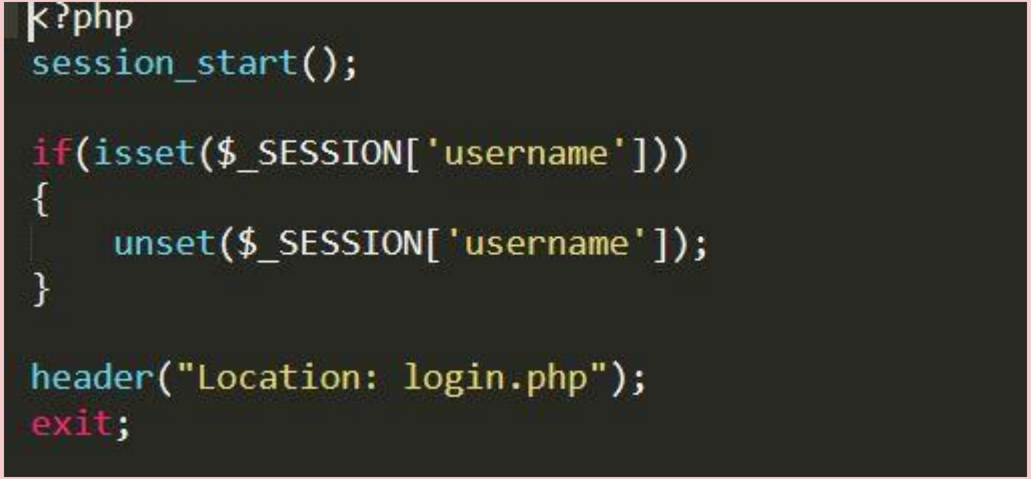
Hello, shiva



```
<!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>
```

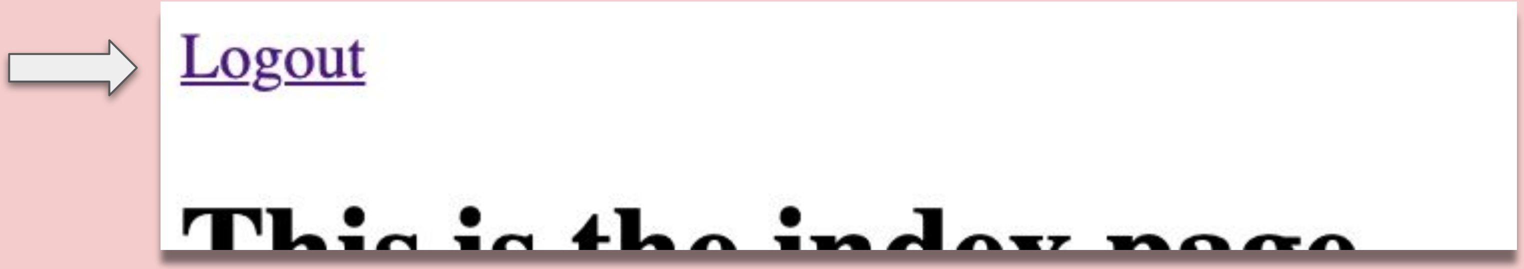
Code: logout.php

- Unsets session username, which is our primary id



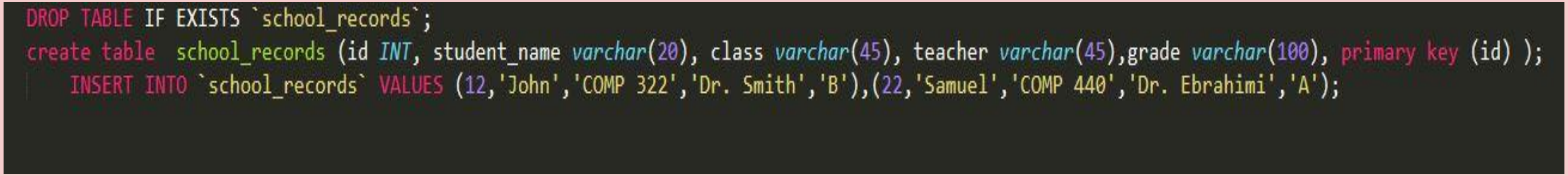
```php
<?php
session_start();

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

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

GUI: logout

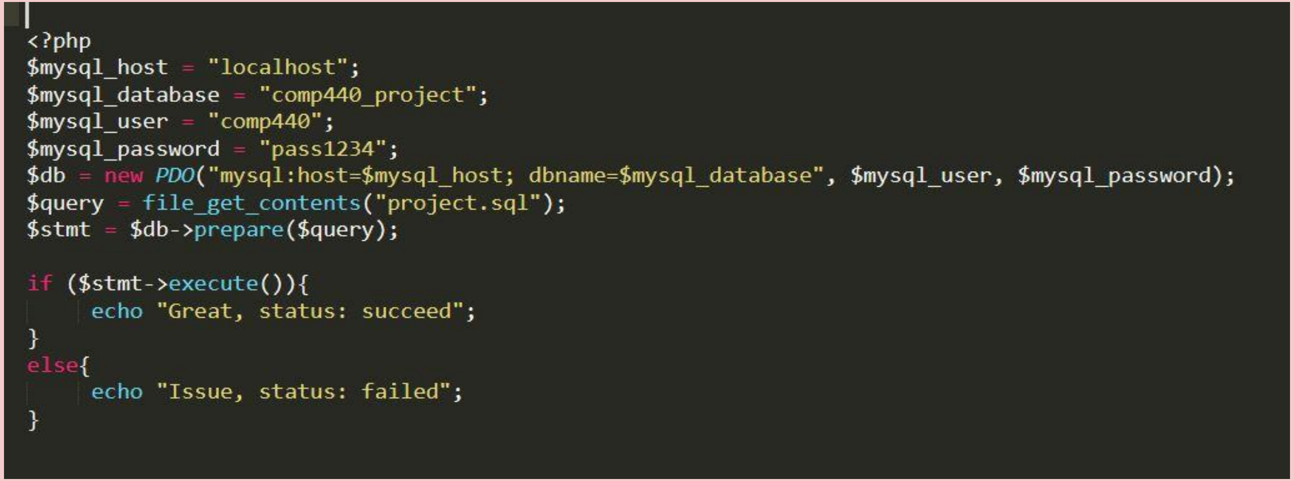


This is the index page

Code : Project.sql && Initializing_database.php

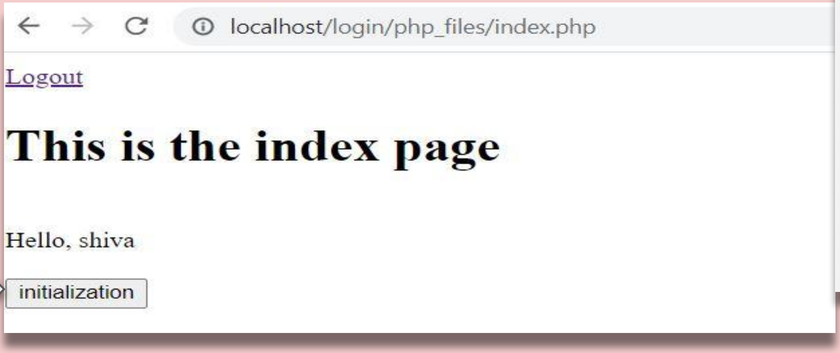


```sql
DROP TABLE IF EXISTS `school_records`;
create table  school_records (id INT, student_name varchar(20), class varchar(45), teacher varchar(45),grade varchar(100), primary key (id) );
    INSERT INTO `school_records` VALUES (12,'John','COMP 322','Dr. Smith','B'),(22,'Samuel','COMP 440','Dr. Ebrahimi','A');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



```php
<?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";
}
```

Output initialization of database

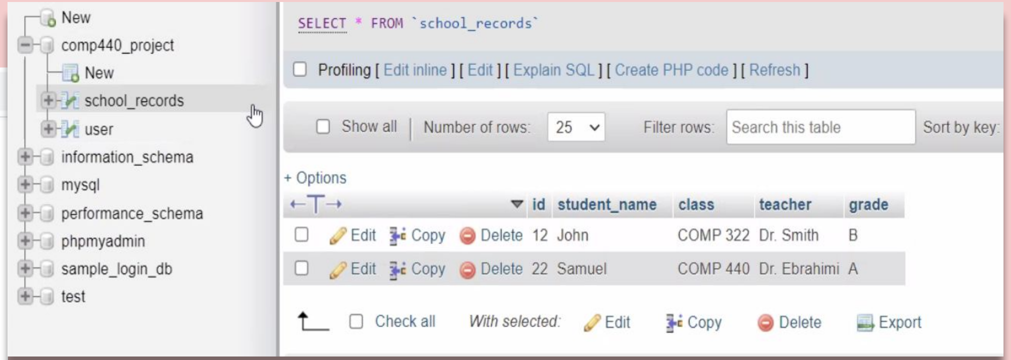


localhost/login/php_files/index.php

Logout

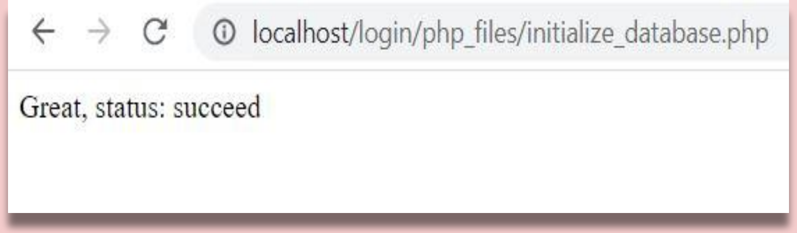
This is the index page

Hello, shiva



```
SELECT * FROM `school_records`
```

	id	student_name	class	teacher	grade
□ Edit Copy Delete	12	John	COMP 322	Dr. Smith	B
□ Edit Copy Delete	22	Samuel	COMP 440	Dr. Ebrahimi	A

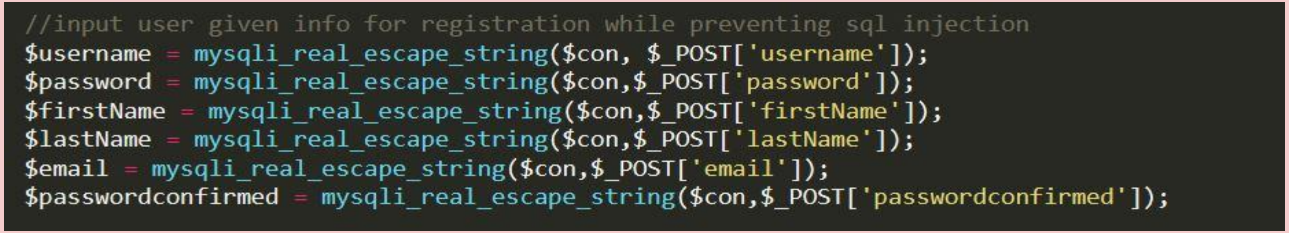


localhost/login/php_files/initialize_database.php

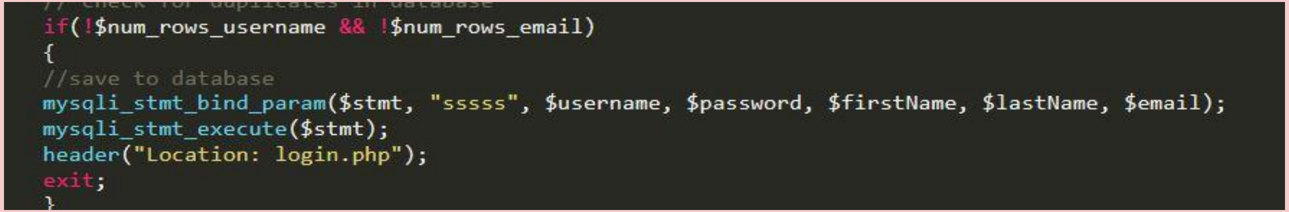
Great, status: succeed

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

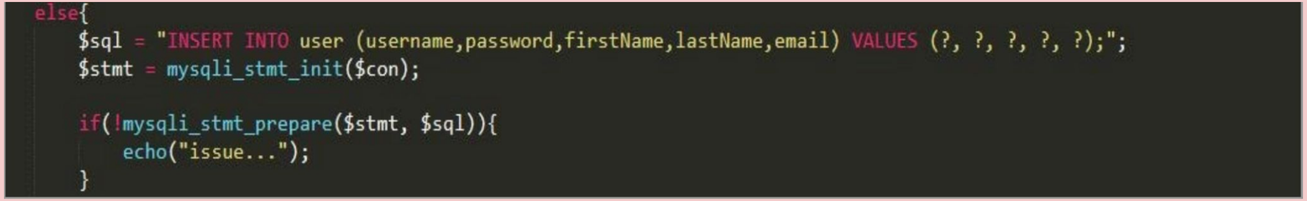
signup.php: SQL Injection Prevention



```php
//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']);
```



```php
// 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;
}
```



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

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