**WEB ENGINEERING**

**ASSIGNMENT # 03**



**SUBMITTED BY:**

Umer Hassan Khan (SP21020)

**SUBMITTED TO:**

MA’AM NABEELA BIBI

**DEPARTMENT OF SOFTWARE ENGINEERING**

**FACULTY OF ENGINEERING & COMPUTER SCIENCES**

**NATIONAL UNIVERSITY OF MODERN LANGUAGES, ISLAMABAD**

**Signup.php**

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

    <title>User Registration</title>

    <script>

        function validateForm() {

            var username = document.forms["signupForm"]["username"].value;

            var email = document.forms["signupForm"]["email"].value;

            var password = document.forms["signupForm"]["password"].value;

            if (username == "" || email == "" || password == "") {

                alert("All fields must be filled out");

                return false;

            }

            return true;

        }

    </script>

</head>

<body>

    <h2>Sign Up</h2>

    <div class="container">

    <form action="register.php" method="post" enctype="multipart/form-data" onsubmit="return validateForm()" name="signupForm">

        <label for="username">Username:</label>

        <input type="text" name="username" required>

        <label for="email">Email:</label>

        <input type="email" name="email" required>

        <label for="password">Password:</label>

        <input type="password" name="password" required>

        <label for="profile\_picture">Profile Picture:</label>

        <input type="file" name="profile\_picture" accept="image/\*">

        <input type="submit" value="Register">

    </form>

    </div>

</body>

</html>

**Register.php**

<?php

include('db\_connection.php');

createConnection();

function sanitizeInput($input) {

    return htmlentities(stripslashes(trim($input)));

}

if ($\_SERVER["REQUEST\_METHOD"] == "POST") {

    // Retrieve user data from the signup form

    $username = sanitizeInput($\_POST["username"]);

    $email = sanitizeInput($\_POST["email"]);

    $password = sanitizeInput($\_POST["password"]);

    $hashedPassword = password\_hash($password, PASSWORD\_DEFAULT);

    $profilePicture = $\_FILES["profile\_picture"];

    $targetDirectory = "uploads/";

    $targetFile = $targetDirectory . basename($profilePicture["name"]);

    move\_uploaded\_file($profilePicture["tmp\_name"], $targetFile);

    $conn = createConnection();

    $checkUserQuery = "SELECT \* FROM user\_table WHERE username = '$username' OR email = '$email'";

    $result = $conn->query($checkUserQuery);

    if ($result->num\_rows > 0) {

        echo "Username or email already exists. Please choose a different one.";

    } else {

        $insertUserQuery = "INSERT INTO user\_table (username, email, password, profile\_picture) VALUES ('$username', '$email', '$hashedPassword', '$targetFile')";

        if ($conn->query($insertUserQuery) === TRUE) {

            echo "Registration successful! You can now <a href='login.php'>login</a>.";

        } else {

            echo "Error: " . $insertUserQuery . "<br>" . $conn->error;

        }

    }

    // Close the database connection

    $conn->close();

}

?>

**Login.php**

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

    <title>Login</title>

</head>

<body>

    <h2>Login</h2>

    <form action="authenticate.php" method="post">

        <label for="username">Username:</label>

        <input type="text" name="username" required><br>

        <label for="password">Password:</label>

        <input type="password" name="password" required><br>

        <input type="submit" value="Login">

    </form>

</body>

</html>

**Authenticate.php**

<?php

include('db\_connection.php');

createConnection();

function sanitizeInput($input) {

    return htmlentities(stripslashes(trim($input)));

}

if ($\_SERVER["REQUEST\_METHOD"] == "POST") {

    $username = sanitizeInput($\_POST["username"]);

    $password = sanitizeInput($\_POST["password"]);

    $conn = createConnection();

    $getUserQuery = "SELECT \* FROM user\_table WHERE username = '$username'";

    $result = $conn->query($getUserQuery);

    if ($result->num\_rows > 0) {

        $row = $result->fetch\_assoc();

        $hashedPassword = $row["password"];

        if (password\_verify($password, $hashedPassword)) {

            // Start a session and set session variables

            session\_start();

            $\_SESSION['user\_id'] = $row['id'];

            header("Location: dashboard.php");

            exit();

        } else {

            echo "Invalid password. Please try again.";

        }

    } else {

        echo "Invalid username. Please try again.";

    }

    $conn->close();

}

?>

**Dashboard.php**

<?php

include('session\_check.php');

$user\_id = $\_SESSION['user\_id'];

echo "Welcome, User with ID $user\_id!";

?>

**Logout.php**

<?php

session\_start();

session\_destroy();

header("Location: login.php");

exit();

?>

**db\_connection.php**

<?php

function createConnection() {

    $hostname = "localhost";

    $username = "root";

    $password = "";

    $database = "user\_registeration ";

    $conn = new mysqli($hostname, $username, $password, $database);

    if ($conn->connect\_error) {

        die("Connection failed: " . $conn->connect\_error);

    }

    return $conn;

}

?>



