<?php

//require("session.php");

session\_start();

if (isset($\_SESSION["user2"])) {

   header("Location: panel\_zafiyetli.php");

}

//require("session.php");

    if (isset($\_POST["login\_button"])) {

        $username = $\_POST["username\_login"];

        $password = $\_POST["password\_login"];

            require\_once "../database/db.php";

            $sql = "SELECT \* FROM users WHERE username = '" . $username . "' AND password = '" . $password . "'";

            //$sql = "SELECT \* FROM users WHERE login = '" . $login . "' AND password = '" . $password . "'";

            $result = mysqli\_query($conn, $sql);

            if ($result === false) {

                // SQL sorgusu başarısız olduysa hata mesajını ekrana yazdır

                echo "SQL Error: " . mysqli\_error($conn);

                die();

            }

            $user2 = mysqli\_fetch\_array($result);

            if ($user2) {

                //if (password\_verify($password, $user["password"])) {

                    //if($username == $user["username"]){

                        //echo "<div class='alert alert-danger'>Password match</div>";

                        //session\_start();

                        $\_SESSION["user2"] = "yes";

                        header("Location: panel\_zafiyetli.php");

                        //echo "<div class='alert alert-danger'>Password match</div>";

                        die();

                    /\* }

                    else{

                    // echo "<div class='alert alert-danger'>Password does not match</div>";

                    // echo $password+" "+$user["password"];

                    //echo $user["username"]." ".$user["password"]." ".$password;

                    }\*/

            }else{

                //echo "<div class='alert alert-danger'>wrong</div>";

            }

        }

        ?>

<?php

        if (isset($\_POST["register\_button"])) {

           $fullName = $\_POST["username\_register"];

           $password = $\_POST["password\_register"];

           //$passwordHash = password\_hash($password, PASSWORD\_DEFAULT);

           $errors = array();

           if (empty($fullName) OR empty($password)) {

            array\_push($errors,"All fields are required");

           }

           /\*

           if (strlen($password)<8) {

            array\_push($errors,"Password must be at least 8 charactes long");

           }

           if ($password!==$passwordRepeat) {

            array\_push($errors,"Password does not match");

           }

           \*/

           require\_once "../database/db.php";

           $sql = "SELECT \* FROM users WHERE username = '$fullName'";

           $result = mysqli\_query($conn, $sql);

           $rowCount = mysqli\_num\_rows($result);

           if ($rowCount>0) {

            array\_push($errors,"username already exists!");

           }

           if (count($errors)>0) {

            foreach ($errors as  $error) {

                echo "<div class='alert alert-danger'>$error</div>";

            }

           }else{

            $sql = "INSERT INTO users (username, password) VALUES ( ?, ?)";

            $stmt = mysqli\_stmt\_init($conn);

            $prepareStmt = mysqli\_stmt\_prepare($stmt,$sql);

            if ($prepareStmt) {

                mysqli\_stmt\_bind\_param($stmt,"ss",$fullName, $password);

                mysqli\_stmt\_execute($stmt);

                echo "<div class='alert alert-success'>You are registered successfully.</div>";

            }else{

                die("Something went wrong");

            }

           }

        }

        ?>

<!DOCTYPE html>

<html>

<head>

    <meta charset=utf-8 />

    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />

    <title> HTML5 lessons </title>

    <link rel="stylesheet" type="text/css" href="../Styles/style.css" />

    <link rel="stylesheet" type="text/css" href="../Styles/sqli/login.css" />

    <link rel="stylesheet" href="../Styles/bootstrap.css">

    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-T3c6CoIi6uLrA9TneNEoa7RxnatzjcDSCmG1MXxSR1GAsXEV/Dwwykc2MPK8M2HN" crossorigin="anonymous">

    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/js/bootstrap.bundle.min.js" integrity="sha384-C6RzsynM9kWDrMNeT87bh95OGNyZPhcTNXj1NW7RuBCsyN/o0jlpcV8Qyq46cDfL" crossorigin="anonymous"></script>

    <script src="https://cdn.jsdelivr.net/npm/@popperjs/core@2.11.8/dist/umd/popper.min.js" integrity="sha384-I7E8VVD/ismYTF4hNIPjVp/Zjvgyol6VFvRkX/vR+Vc4jQkC+hVqc2pM8ODewa9r" crossorigin="anonymous"></script>

    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/js/bootstrap.min.js" integrity="sha384-BBtl+eGJRgqQAUMxJ7pMwbEyER4l1g+O15P+16Ep7Q9Q+zqX6gSbd85u4mG4QzX+" crossorigin="anonymous"></script>

</head>

<body>

    <script src="../Js/bootstrap.js"></script>

    <main>

        <?php require("../header.php") ?>

        <div class="col mt-2 mb-2">

            <div class="d-flex flex-column-reverse align-items-center">

                    <div class="mainText px-2">

    <h1>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;

    SQL Injection Lab

    &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;

    </h1>

    <h1>

    &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;

    (Vulnerable)

    &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;

    </h1>

    <div class="container">

        <div class="sign-in">

            <h2>Sign In</h2>

            <form action="login\_zafiyetli.php" method="post">

                <input type="text" placeholder="Username" name="username\_login" class="form-control" required>

                <input type="password" placeholder="Password" name="password\_login" class="form-control" required>

                <button type="submit" name="login\_button">Sign In</button>

            </form>

        </div>

        <div class="sign-up">

            <h2>Sign Up</h2>

            <form action="login\_zafiyetli.php" method="POST">

                <input type="text" placeholder="Username" name="username\_register" required>

                <input type="password" placeholder="Password" name="password\_register" required>

                <button type="submit" name="register\_button">Sign Up</button>

            </form>

        </div>

    </div>

                    </div>

            </div>

        </div>

        <footer class="page-bottom">

        <button class="primary" onclick="window.dialog.showModal();">Show Hint</button>

        <dialog id="dialog" class="dialog">

            <h2>Walkthrough</h2>

            <h4>Steps</h4>

            <li>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus efficitur faucibus nisi. Mauris quis velit a eros dignissim accumsan. Fusce auctor ex est, sed ultricies urna feugiat vitae. Sed magna risus, facilisis ac turpis in, semper pharetra neque. Nam a ante accumsan nisl vehicula feugiat. Nam nisi neque, mattis eu tellus quis, facilisis porttitor metus. Quisque tempus tempor massa, vitae tincidunt elit tristique ac. Donec molestie sapien et quam mollis, vel gravida massa laoreet. Aliquam at felis volutpat, auctor tellus a, dignissim mauris. Sed convallis eros sit amet lorem auctor, id tincidunt nulla auctor</li>

            <li>123</li>

            <li>123</li>

            <p><a href="#">Tutorial Video</a></p>

            <button onclick="window.dialog.close();" aria-label="close" class="x">❌</button>

        </dialog>

         <div class="d-flex flex-row gap-2">

         <div class="btn-group">

         <button class="btn btn-secondary dropdown-toggle" type="button" data-bs-toggle="dropdown" data-bs-auto-close="false" aria-expanded="false">

             Zafiyet Durumu

         </button>

         <ul class="dropdown-menu">

             <li><a class="dropdown-item" href="login\_zafiyetsiz.php">Zafiyetsiz</a></li>

             <li><a class="dropdown-item" href="login\_zafiyetli.php">Zafiyetli</a></li>

         </ul>

        </div>

             <div class="square">SQLi</br>(Zafiyetsiz)</div>

        </div>

        </footer>

    </main>

</body>

</html>