Source code to Markdown

This file is automatically created by a script. Please delete this line and replace with the course and your team information accordingly. ## updateuser.php

```
<?php
    require "database.php";
    $username = $_POST["username"];
    $fullName = $_POST["fullName"];
    $email = $_POST["email"];
    $password = $_POST["password"];
    $phoneNumber = $_POST["phoneNumber"];
    if(isset($username) && isset($password) && isset($fullName) && isset($email) && isset($p
        if(updateuser($username, $fullName, $email, $password, $phoneNumber)){
            echo "Profile Update Succeeded";
        }else{
            echo "Profile Update Failed!";
        }
    }
    else{
        echo "No username/password/email/phoneNumber/fullName provided!";
    }
?>
<form action="form.php" method="GET">
    <button type="submit">Go back to login page</button>
</form>
```

form.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Login Form</title>
  <link rel="stylesheet" href="styles.css">
</head>
<body>
  <div class="container">
    <div class="card">
      <h1>TEAM 01 - WAPH</h1>
      <h2>Login</h2>
      <form action="index.php" method="POST" class="form login">
        <div class="input-group">
          <label for="username">Username:</label>
          <input type="text" class="text_field" name="username" id="username" placeholder="E
        </div>
        <div class="input-group">
          <label for="password">Password:</label>
          <input type="password" class="text_field" name="password" id="password" placeholde
        </div>
        <button class="button" type="submit">Login</button>
      </form>
      <div class="registration-link">
        <span>Don't have an account?</span>
        <button class="button" onclick="window.location.href='registrationform.php';">Regist
      </div>
    </div>
  </div>
</body>
</html>
```

addnewuser.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Registration Status</title>
  <link rel="stylesheet" href="styles.css">
</head>
<body>
<div class="container">
  <div class="card">
    <h2>Registration Status</h2>
    <?php
      require "database.php";

      function sanitizeInput($data) {
        $data = trim($data);
        $data = stripslashes($data);
        $data = htmlspecialchars($data);
        return $data;
      }

      $username = isset($_POST["username"]) ? sanitizeInput($_POST["username"]) : "";
      $fullName = isset($_POST["fullName"]) ? sanitizeInput($_POST["fullName"]) : "";
      $email = isset($_POST["email"]) ? sanitizeInput($_POST["email"]) : "";
      $password = isset($_POST["password"]) ? sanitizeInput($_POST["password"]) : "";
      $phoneNumber = isset($_POST["phoneNumber"]) ? sanitizeInput($_POST["phoneNumber"]) : "
```

```
   $errors = [];
   if (empty($username) || empty($fullName) || empty($email) || empty($password) || empty
    $errors[] = "All fields are required!";
   }
   if (!filter_var($email, FILTER_VALIDATE_EMAIL)) {
    $errors[] = "Invalid email format!";
   }
   if (!preg_match("/^[0-9]{10}$/", $phoneNumber)) {
    $errors[] = "Invalid phone number format!";
   }
   if (strlen($password) < 8) {
    $errors[] = "Password must be at least 8 characters long!";
   }

   if (empty($errors)) {
    if (addnewuser($username, $fullName, $email, $password, $phoneNumber)) {
     echo "<p>Registration Succeeded</p>";
    } else {
     echo "<p>Registration Failed!</p>";
    }
   } else {
    foreach ($errors as $error) {
     echo "<p class='error'>" . $error . "</p>";
    }
   }
  ?>
  <form action="form.php" method="GET">
   <button type="submit" class="button">Go back to login page</button>
  </form>
 </div>
</div>
</body>
</html>
```

insertpost.php

```
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <meta name="viewport" content="width=device-width, initial-scale=1.0">
 <title>Add a New Post</title>
 <link rel="stylesheet" href="styles.css">
</head>
<body>
 <div class="container">
```

```
    <div class="card">
      <?php
      require "sessionauthentication.php";
      require "database.php";

      if (isset($_POST['postContent'])) {
          $postContent = htmlspecialchars($_POST['postContent']);
          $username = $_SESSION['username'];

          if (insertPost($postContent, $username)) {
              echo "<h2>Success</h2><p>Post added successfully.</p>";
          } else {
              echo "<h2>Error</h2><p>Failed to add post.</p>";
          }
      } else {
          echo "<h2>Error</h2><p>No post content provided.</p>";
      }
      header("Refresh:2; url=index.php");
      ?>
    </div>
  </div>
</body>
</html>
```

deletepost.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Delete Post</title>
  <link rel="stylesheet" href="styles.css">
</head>
<body>
  <div class="container">
    <div class="card">
      <?php
      require "sessionauthentication.php";
      require "database.php";

      if (!isset($_POST['postID'])) {
          echo "<h2>Error</h2><p>Post ID not provided.</p>";
          die();
      }
      $postID = $_POST['postID'];

      if (deletePost($postID)) {
          echo "<h2>Success</h2><p>Post deleted successfully.</p>";
      } else {
          echo "<h2>Error</h2><p>Failed to delete post.</p>";
      }

      header("Refresh:2; url=index.php");
      ?>
    </div>
  </div>
</body>
</html>
```

viewprofile.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>View Profile - WAPH</title>
  <link rel="stylesheet" href="styles.css">
</head>
<body>
  <div class="container">
    <div class="view-profile-card">
      <h1>View User Profile - WAPH</h1>
      <div id="digit-clock"></div>

      <?php
      session_start();
      require "database.php";

      if (isset($_SESSION['username'])) {
        $userProfile = fetchUserProfile($_SESSION['username']);

        if ($userProfile) {
          ?>
          <form name="viewProfileForm" action="#" method="GET" class="form view-profile">
            <div class="input-group">
              <label for="username">Username:</label>
              <input type="text" class="text_field" name="username" value="<?= htmlentities
            </div>
            <div class="input-group">
```

```
              <label for="fullName">Full Name:</label>
              <input type="text" class="text_field" name="fullName" value="<?= htmlentities(
            </div>
            <div class="input-group">
              <label for="email">Email:</label>
              <input type="email" class="text_field" name="email" value="<?= htmlentities($u
            </div>
            <div class="input-group">
              <label for="phoneNumber">Phone Number:</label>
              <input type="tel" class="text_field" name="phoneNumber" value="<?= htmlentitie
            </div>
          </form>
          <?php
        } else {
          echo '<p>No profile found for the current user.</p>';
        }
      } else {
        echo '<p>User is not logged in.</p>';
      }
      ?>

      <form id="editUserForm" action="edituser.php" method="POST">
        <input type="hidden" name="username" value="<?= isset($_SESSION['username']) ? htmle
        <button class="button" type="submit">Edit Profile</button>
      </form>
      <form action="index.php" method="POST">
        <button class="button" type="submit">Go Back</button>
      </form>
    </div>
  </div>
</body>
</html>
```

addpost.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Add a New Post</title>
  <link rel="stylesheet" href="styles.css">
</head>
<body>
  <div class="container">
    <div class="card">
```

```
      <h2>Add a New Post</h2>
      <form action="insertpost.php" method="POST" class="form login">
        <div class="input-group">
          <label for="postContent">Post Content:</label>
          <textarea name="postContent" rows="4" cols="50" class="text_field" required></text
        </div>
        <button class="button" type="submit">Post</button>
        <button class="button" onclick="window.location.href='index.php';">Home</button>
      </form>
    </div>
  </div>
</body>
</html>
```

sessionauthentication.php

```
<?php
session_set_cookie_params(15*60, "/", "waph-team01.minifacebook.com", TRUE, TRUE);
session_start();

if (!isset($_SESSION['authenticated']) || $_SESSION['authenticated'] !== TRUE) {
    session_destroy();
    echo "<script>alert('You have not logged in. Please login first');</script>";
    header("Refresh:0; url=form.php");
    die();
}


if ($_SESSION["browser"] !== $_SERVER["HTTP_USER_AGENT"]) {
    session_destroy();
    echo "<script>alert('Session hijacking attack is detected!');</script>";
    header("Refresh:0; url=form.php");
    die();
}
?>
```

edituser.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Edit Profile - WAPH</title>
  <link rel="stylesheet" href="styles.css">
</head>
```

```
<body>
  <div class="container">
    <div class="edit-profile-card">
      <h1>Edit User Profile - WAPH</h1>
      <form name="editProfileForm" action="updateuser.php" method="POST" class="form edit-pr
        <div class="input-group">
          <label for="username">Username:</label>
          <input type="text" class="text_field" name="username" value="<?php session_start()
        </div>
        <div class="input-group">
          <label for="fullName">Full Name:</label>
          <input type="text" class="text_field" name="fullName" required oninput="validateFu
          <div class="error-message" id="fullName-error"></div>
        </div>
        <div class="input-group">
          <label for="email">Email:</label>
          <input type="email" class="text_field" name="email" required placeholder="username
          <div class="error-message" id="email-error"></div>
        </div>
        <div class="input-group">
          <label for="password">Password:</label>
          <input type="password" class="text_field" name="password" required oninput="valida
          <div class="error-message" id="password-error"></div>
        </div>
        <div class="input-group">
          <label for="phoneNumber">Phone Number:</label>
          <input type="tel" class="text_field" name="phoneNumber" required pattern="[0-9]{10
          <div class="error-message" id="phoneNumber-error"></div>
        </div>
        <button class="button" type="button" onclick="window.location.href='index.php';">Hom
        <button class="button" type="submit">Update Profile</button>
      </form>
    </div>
  </div>

  <script>
    // Function to validate full name
    function validateFullName() {
      var fullName = document.forms["editProfileForm"]["fullName"].value;
      var fullNameError = document.getElementById("fullName-error");
      if (fullName.trim() === "") {
        fullNameError.innerHTML = "Full Name must be filled out";
      } else {
        fullNameError.innerHTML = "";
      }
    }
```

```
// Function to validate email
function validateEmail() {
  var email = document.forms["editProfileForm"]["email"].value;
  var emailError = document.getElementById("email-error");
  if (email.trim() === "") {
    emailError.innerHTML = "Email must be filled out";
  } else {
    emailError.innerHTML = "";
  }
}

// Function to validate password
function validatePassword() {
  var password = document.forms["editProfileForm"]["password"].value;
  var passwordError = document.getElementById("password-error");
  if (password.trim() === "") {
    passwordError.innerHTML = "Password must be filled out";
  } else {
    passwordError.innerHTML = "";
  }
}

// Function to validate phone number
function validatePhoneNumber() {
  var phoneNumber = document.forms["editProfileForm"]["phoneNumber"].value;
  var phoneNumberError = document.getElementById("phoneNumber-error");
  if (phoneNumber.trim() === "") {
    phoneNumberError.innerHTML = "Phone Number must be filled out";
  } else {
    phoneNumberError.innerHTML = "";
  }
}

// Function to validate the entire form
function validateForm() {
  validateFullName();
  validateEmail();
  validatePassword();
  validatePhoneNumber();

  var errors = document.querySelectorAll(".error-message");
  for (var i = 0; i < errors.length; i++) {
    if (errors[i].innerHTML !== "") {
      return false;
    }
```

```
      }

      return true;
    }

    // Add event listeners to input fields for instant validation
    document.getElementsByName("fullName")[0].addEventListener("input", validateFullName);
    document.getElementsByName("email")[0].addEventListener("input", validateEmail);
    document.getElementsByName("password")[0].addEventListener("input", validatePassword);
    document.getElementsByName("phoneNumber")[0].addEventListener("input", validatePhoneNumb
  </script>
</body>
</html>
```

addcomment.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Add Comment</title>
  <link rel="stylesheet" href="styles.css">
  <style>
    .container {
      display: flex;
      justify-content: center;
      align-items: center;
      height: 100vh;
    }

    .card {
      max-width: 90%;
      width: 400px;
      padding: 20px;
      border-radius: 8px;
      background-color: #f9f9f9;
      box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
    }

    .card h2 {
      margin-top: 0;
    }

    .card form {
      margin-top: 20px;
    }

    .card textarea {
      width: calc(100% - 20px);
      padding: 10px;
      border: 1px solid #ccc;
      border-radius: 4px;
      resize: vertical;
      margin-bottom: 10px;
    }

    .card input[type="submit"] {
      background-color: #007bff;
      color: #fff;
      border: none;
      padding: 10px 20px;
      border-radius: 4px;
      cursor: pointer;
    }

    .card input[type="submit"]:hover {
      background-color: #0056b3;
    }
  </style>
</head>
<body>
  <div class="container">
    <div class="card">
      <h2>Add Comment</h2>
      <?php
      require "sessionauthentication.php";
      require "database.php";

      if (isset($_POST['commentContent']) && isset($_POST['postID'])) {
          $commentContent = htmlspecialchars($_POST['commentContent']);
          $postID = $_POST['postID'];
          $username = $_SESSION['username'];

          if (insertComment($commentContent, $postID, $username)) {
              echo "Comment added successfully.";
          } else {
              echo "Failed to add comment.";
          }
      } else {
          echo "No comment content was provided";
      }
      header("Refresh:2; url=index.php");
      ?>
    </div>
  </div>
</body>
</html>
```

registrationform.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Registration Form</title>
  <link rel="stylesheet" href="styles.css">
</head>
<body>
  <div class="container">
    <div class="card">
      <h2>New User Registration</h2>
      <div id="digit-clock"></div>
      <form name="registrationForm" action="addnewuser.php" method="POST" class="form login"
        <div class="input-group">
          <label for="username">Username:</label>
          <input type="text" class="text_field" name="username" id="username" required place
          <div id="username-error" class="error-message">Username is required</div>
        </div>
        <div class="input-group">
          <label for="fullName">Full Name:</label>
          <input type="text" class="text_field" name="fullName" id="fullName" required>
          <div id="fullName-error" class="error-message"></div>
        </div>
        <div class="input-group">
          <label for="email">Email:</label>
          <input type="email" class="text_field" name="email" id="email" required pattern="
          <div id="email-error" class="error-message">Invalid email format</div>
        </div>
        <div class="input-group">
          <label for="password">Password:</label>
          <input type="password" class="text_field" name="password" id="password" required c
          <div id="password-error" class="error-message"></div>
        </div>
        <div class="input-group">
          <label for="confirmPassword">Confirm Password:</label>
          <input type="password" class="text_field" name="confirmPassword" id="confirmPasswo
          <div id="confirmPassword-error" class="error-message">Passwords do not match</div
        </div>
        <div class="input-group">
          <label for="phoneNumber">Phone Number:</label>
          <input type="tel" class="text_field" name="phoneNumber" id="phoneNumber" required
          <div id="phoneNumber-error" class="error-message">Invalid phone number format</di
        </div>
        <button class="button" type="submit">Register</button>
        <button class="button" onclick="window.location.href='form.php';">Go back</button>
      </form>
    </div>
  </div>
  <script>
    function validateEmail(input) {
      var isValid = /^[^\s@]+@[^\s@]+\.[^\s@]+$/.test(input.value);
      var errorElement = document.getElementById("email-error");
      if (!isValid) {
        errorElement.style.display = "block";
      } else {
        errorElement.style.display = "none";
      }
    }

    function validatePhoneNumber(input) {
      var isValid = /^\d{10}$/.test(input.value);
      var errorElement = document.getElementById("phoneNumber-error");
      if (!isValid) {
        errorElement.style.display = "block";
      } else {
        errorElement.style.display = "none";
      }
    }

    function validatePassword(input) {
      var password = input.value;
      var errorElement = document.getElementById("password-error");

      var strongPasswordRegex = /^(?=.*\d)(?=.*[a-z])(?=.*[A-Z])(?=.*[^\da-zA-Z])(?!.*\s).{

      if (!strongPasswordRegex.test(password)) {
        errorElement.textContent = "Password must be at least 8 characters and include a nu
        errorElement.style.display = "block";
      } else {
        errorElement.style.display = "none";
      }
    }

    function validatePasswordMatch(input) {
      var password = document.getElementById("password").value;
      var confirmPassword = input.value;
      var errorElement = document.getElementById("confirmPassword-error");
      if (password !== confirmPassword) {
        errorElement.style.display = "block";
      } else {
        errorElement.style.display = "none";
      }
    }

    function validateForm() {
      var isValid = true;
      var inputs = document.querySelectorAll("input");
      inputs.forEach(function(input) {
        if (!input.checkValidity()) {
          isValid = false;
          input.reportValidity();
        }
      });
      return isValid;
    }
  </script>
</body>
</html>
```

logout.php

```
<?php
session_start();

if(isset($_SESSION['user_id'])) {
    session_destroy();
}
header("Location: form.php");
exit;
?>
```

database.php

```
<?php
$mysqli = new mysqli('localhost', 'team01', 'Pa$$w0rd', 'waph_team');
if ($mysqli->connect_errno) {
    printf("Database connection failed: %s\n", $mysqli->connect_error);
    return false;
}

function addnewuser($username, $fullname, $otheremail, $password, $phone) {
    global $mysqli;
    $prepared_sql = "INSERT INTO users(username, password, fullname, otheremail, phone) VALU
    $stmt = $mysqli->prepare($prepared_sql);
    $stmt->bind_param("sssss", $username, $password, $fullname, $otheremail, $phone);
    if ($stmt->execute()) return true;
    return false;
}

function updateuser($username, $fullname, $otheremail, $password, $phone) {
    global $mysqli;
    $prepared_sql = "UPDATE users SET password=md5(?), fullname=?, otheremail=?, phone=? WHE
    $stmt = $mysqli->prepare($prepared_sql);
    $stmt->bind_param("sssss", $password, $fullname, $otheremail, $phone, $username);
    if ($stmt->execute()) return true;
    return false;
}

function fetchUserProfile($username)
{
    global $mysqli;
    $prepared_sql = "SELECT * FROM users WHERE username = ?";
    $stmt = $mysqli->prepare($prepared_sql);
    $stmt->bind_param("s", $username);
    $stmt->execute();
    $result = $stmt->get_result();
    if ($result->num_rows === 1) {
        return $result->fetch_assoc();
    }
    return null;
}

function checklogin_mysql($username, $password) {
    global $mysqli;
    $prepared_sql = "SELECT * FROM users WHERE username = ? AND password = MD5(?) AND accoun
    $stmt = $mysqli->prepare($prepared_sql);
    $stmt->bind_param("ss", $username, $password);
    $stmt->execute();
    $result = $stmt->get_result();
    if ($result->num_rows >= 1) return true;
    return false;
}
```

```
function changepassword($username, $password) {
    global $mysqli;
    $prepared_sql = "UPDATE users SET password = md5(?) WHERE username= ?";
    $stmt = $mysqli->prepare($prepared_sql);
    $stmt->bind_param("ss", $password, $username);
    if ($stmt->execute()) return true;
    return false;
}

function editUser($username, $fullname, $otheremail, $phone) {
    global $mysqli;
    $prepared_sql = "UPDATE users SET fullname = ?, otheremail = ?, phone = ? WHERE username
    $stmt = $mysqli->prepare($prepared_sql);
    $stmt->bind_param("ssss", $fullname, $otheremail, $phone, $username);
    return $stmt->execute();
}

function insertPost($postContent, $username) {
    global $mysqli;
    $prepared_sql = "INSERT INTO posts (postContent, postDate, username) VALUES (?, NOW(), ?
    $stmt = $mysqli->prepare($prepared_sql);
    $stmt->bind_param("ss", $postContent, $username);
    return $stmt->execute();
}

function insertComment($commentContent, $postID, $username) {
    global $mysqli;
    $prepared_sql = "INSERT INTO comments (commentContent, commentDate, postID, username) VA
    $stmt = $mysqli->prepare($prepared_sql);
    $stmt->bind_param("sis", $commentContent, $postID, $username);
    return $stmt->execute();
}

function updatePost($postID, $postContent) {
    global $mysqli;
    $prepared_sql = "UPDATE posts SET postContent = ? WHERE postID = ?";
    $stmt = $mysqli->prepare($prepared_sql);
    $stmt->bind_param("si", $postContent, $postID);
    return $stmt->execute();
}

function deletePost($postID) {
    global $mysqli;
    $prepared_sql = "DELETE FROM posts WHERE postID = ?";
    $stmt = $mysqli->prepare($prepared_sql);
    $stmt->bind_param("i", $postID);
    return $stmt->execute();
}

function changeUserStatus($username, $status) {
    global $mysqli;
    $prepared_sql = "UPDATE users SET account_enabled = ? WHERE username = ?";
    $stmt = $mysqli->prepare($prepared_sql);
    $stmt->bind_param("is", $status, $username);
    return $stmt->execute();
}

?>
```

changepasswordform.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Change Password Form</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color:#f0fff0;
      margin: 0;
      padding: 0;
    }

    .container {
      max-width: 600px;
      margin: 50px auto;
      background-color: #fff;
      padding: 20px;
      border-radius: 10px;
      box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
      text-align: center;
    }

    h1 {
      font-size: 24px;
      margin-bottom: 20px;
    }

    .form {
      text-align: left;
    }

    .input-group {
      margin-bottom: 20px;
    }

    .input-group label {
      display: block;
      margin-bottom: 5px;
      font-weight: bold;
    }

    .input-group input {
      width: 100%;
      padding: 10px;
      border-radius: 5px;
      border: 1px solid #ccc;
      box-sizing: border-box;
    }

    .button {
      display: inline-block;
      padding: 10px 20px;
      margin-right: 10px;
      background-color: #4CAF50;
      color: white;
      border: none;
      border-radius: 5px;
      cursor: pointer;
      transition: background-color 0.3s;
    }

    .button:hover {
      background-color: #45a049;
    }

    .error-message {
      color: red;
      font-size: 12px;
      margin-top: 5px;
    }
  </style>
</head>
<body>
  <div class="container">
    <?php
    session_start();
    require "sessionauthentication.php";
    $rand = bin2hex(openssl_random_pseudo_bytes(16));
    $_SESSION["nocsrftoken"] = $rand;
    ?>
    <h1>Change Password Form</h1>
    <form action="changepassword.php" method="POST" class="form login" onsubmit="return vali
      <div class="input-group">
        <label for="username">Username:</label>
        <input type="text" class="text_field" name="username" value="<?php echo isset($_SESS
      </div>
      <div class="input-group">
        <label for="password">Current Password:</label>
        <input type="password" class="text_field" name="password" />
      </div>
      <div class="input-group">
        <label for="newpassword">New Password:</label>
        <input type="password" class="text_field" name="newpassword" id="newpassword" oninpu
        <div class="error-message" id="newpassword-error"></div>
      </div>
      <div class="input-group">
        <label for="confirmpassword">Confirm New Password:</label>
        <input type="password" class="text_field" name="confirmpassword" id="confirmpasswor
        <div class="error-message" id="confirmpassword-error"></div>
      </div>
      <div>
        <input type="hidden" name="nocsrftoken" value="<?php echo $rand; ?>"/>
      </div>
      <button class="button" type="submit">Change password</button>
      <button class="button" onclick="window.location.href='index.php';">Home</button>
    </form>
  </div>

  <script>
    function validatePassword() {
      var newPassword = document.getElementById("newpassword").value;
      var confirmPassword = document.getElementById("confirmpassword").value;
      var newPasswordError = document.getElementById("newpassword-error");
      var confirmPasswordError = document.getElementById("confirmpassword-error");

      // Check if passwords match
      if (newPassword !== confirmPassword) {
        confirmPasswordError.textContent = "Passwords do not match.";
        return false;
      }
```

```
   // Check password format
   if (newPassword.length < 8 || !/[A-Z]/.test(newPassword) || !/[!@#$%^&*()_+\-=\[\]{};
    newPasswordError.textContent = "Password must be at least 8 characters long and cont
    return false;
   }

   // Clear error messages
   newPasswordError.textContent = "";
   confirmPasswordError.textContent = "";

   return true;
  }

  function checkPasswordFormat(input) {
   var newPassword = input.value;
   var newPasswordError = document.getElementById("newpassword-error");

   if (newPassword.length < 8 || !/[A-Z]/.test(newPassword) || !/[!@#$%^&*()_+\-=\[\]{};
    newPasswordError.textContent = "Password must be at least 8 characters long and cont
   } else {
    newPasswordError.textContent = "";
   }
  }

  function checkPasswordMatch() {
   var newPassword = document.getElementById("newpassword").value;
   var confirmPassword = document.getElementById("confirmpassword").value;
   var confirmPasswordError = document.getElementById("confirmpassword-error");

   if (newPassword !== confirmPassword) {
    confirmPasswordError.textContent = "Passwords do not match.";
   } else {
    confirmPasswordError.textContent = "";
   }
  }
 </script>
</body>
</html>
```

index.php

```
<?php
session_set_cookie_params(15*60, "/", "waph-team01.mini.facebook.com", TRUE, TRUE);
session_start();

require_once "database.php";
```

```
if (isset($_POST["username"]) && isset($_POST["password"])) {
    $username = $_POST["username"];
    $password = $_POST["password"];

    if (checklogin_mysql($username, $password)) {
        $_SESSION["authenticated"] = TRUE;
        $_SESSION["username"] = $username;
        $_SESSION["browser"] = $_SERVER["HTTP_USER_AGENT"];
    } else {
        session_destroy();
        echo "<script>alert('Invalid Username or password please recheck');window.location=
        die();
    }
}

if (!isset($_SESSION["authenticated"]) || $_SESSION["authenticated"] != TRUE) {
    session_destroy();
    echo "<script>alert('You have not logged in. Please login first');</script>";
    header("Refresh:0; url=form.php");
    die();
}

if ($_SESSION["browser"] != $_SERVER["HTTP_USER_AGENT"]) {
    session_destroy();
    echo "<script>alert('Session hijack detected')</script>";
    header("Refresh:0; url=form.php");
    die();
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Welcome Page</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color: #f0fff0;
    }

    .container {
      text-align: center;
      padding-top: 20px;
    }
```

```
.welcome-text {
  font-size: 24px;
  font-weight: bold;
  margin-bottom: 20px;
}

.links {
  display: flex;
  justify-content: center;
  align-items: center;
  flex-wrap: wrap;
}

.links form {
  margin: 10px;
}

.links button {
  padding: 10px 20px;
  font-size: 16px;
  cursor: pointer;
  background-color: #4CAF50; /* Green */
  color: white;
  border: none;
  border-radius: 5px;
  transition: background-color 0.3s;
}

.links button:hover {
  background-color: #45a049; /* Darker green on hover */
}

.post-container {
  margin-bottom: 20px;
}

.post {
  background-color: #f9f9f9;
  border-radius: 8px;
  padding: 20px;
}

.post h3 {
  margin-top: 0;
}
```

```
.post p {
  margin-bottom: 10px;
}

.comment {
  background-color: #f0f0f0;
  border-radius: 4px;
  padding: 10px;
  margin-top: 10px;
}

.comment p {
  margin-bottom: 5px;
}

.add-comment-form {
  margin-top: 10px;
}

.add-comment-form textarea {
  width: calc(100% - 20px);
  padding: 10px;
  border: 1px solid #ccc;
  border-radius: 4px;
  resize: vertical;
  margin-bottom: 10px;
}

.add-comment-form input[type="submit"] {
  background-color: #4CAF50; /* Green */
  color: white;
  border: none;
  padding: 10px 20px;
  border-radius: 4px;
  cursor: pointer;
  transition: background-color 0.3s;
}

.add-comment-form input[type="submit"]:hover {
  background-color: #45a049; /* Darker green on hover */
}

/* Adjust home button color */
button[type="submit"] {
  background-color: #4CAF50; /* Green */
```

```
   color: white;
   border: none;
   padding: 10px 20px;
   border-radius: 4px;
   cursor: pointer;
   transition: background-color 0.3s;
  }

  button[type="submit"]:hover {
   background-color: #45a049; /* Darker green on hover */
  }

  .edit-delete-container {
   display: inline-block;
  }

  .edit-post-form, .delete-post-form {
   display: inline;
  }
 </style>
</head>
<body>
 <div class="container">
   <?php
   echo "<div class='welcome-text'>Welcome " . htmlentities($_SESSION['username']) . "!</
   ?>
   <div class="links">
     <form id="addpostform" action="addpost.php" method="POST">
     <button type="submit">Add Post</button>
      </form>
    <form id="changepasswordform" action="changepasswordform.php" method="POST">
     <input type="hidden" name="username" value="<?php echo urlencode($_SESSION['userna
     <button type="submit">Change Password</button>
    </form>
    <form id="viewprofileform" action="viewprofile.php" method="POST">
     <input type="hidden" name="username" value="<?php echo urlencode($_SESSION['userna
     <button type="submit">View/Edit Profile</button>
    </form>
    <form id="usermanagementform" action="usermanagement.php" method="POST">
    <button type="submit">User Management</button>
    </form>
    <form id="logout" action="logout.php" method="POST">
     <button type="submit">Logout</button>
    </form>
  </div>
```

```
<h1>Posts</h1>

<?php
$posts = $mysqli->query("SELECT p.postID, p.postContent, p.postDate, u.username
                         FROM posts p
                         JOIN users u ON p.username = u.username
                         ORDER BY p.postDate DESC");

if ($posts->num_rows > 0) {
    while ($row = $posts->fetch_assoc()) {
        echo "<div class='post-container'>";
        echo "<div class='post'>";
        echo "<h3>" . htmlspecialchars($row['username']) . " posted on " . $row['postDat
        echo "<p>" . htmlspecialchars($row['postContent']) . "</p>";

        echo "<div class='edit-delete-container'>";
        if ($row['username'] == $_SESSION['username']) {
            echo "<form action='editpost.php' method='POST' class='edit-post-form edit-
            echo "<input type='hidden' name='postID' value='" . $row['postID'] . "'>";
            echo "<button type='submit'>Edit</button>";
            echo "</form>";
            echo "<form action='deletepost.php' method='POST' class='delete-post-form ed
            echo "<input type='hidden' name='postID' value='" . $row['postID'] . "'>";
            echo "<button type='submit'>Delete</button>";
            echo "</form>";
        }
        echo "</div>";

        echo "<h4>Comments:</h4>";

        $comments = $mysqli->query("SELECT c.commentContent, c.commentDate, u.username
                                    FROM comments c
                                    JOIN users u ON c.username = u.username
                                    WHERE c.postID = " . $row['postID'] . "
                                    ORDER BY c.commentDate ASC");

        if ($comments->num_rows > 0) {
            while ($commentRow = $comments->fetch_assoc()) {
                echo "<div class='comment'>";
                echo "<p>" . htmlspecialchars($commentRow['username']) . " commented on
                echo "<p>" . htmlspecialchars($commentRow['commentContent']) . "</p>";
                echo "</div>";
            }
        }

        echo "<h4>Add a Comment:</h4>";
```

```
            echo "<form action='addcomment.php' method='POST' class='add-comment-form'>";
            echo "<textarea name='commentContent' rows='2' required></textarea>";
            echo "<input type='hidden' name='postID' value='" . $row['postID'] . "'>";
            echo "<input type='submit' value='Comment'>";
            echo "</form>";
            echo "</div>";
            echo "</div>";
        }
    } else {
        echo "<p>No posts found.</p>";
    }
    ?>
  </div>
</body>
</html>
```

changepassword.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Change Password Form</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color: #f0f0f0;
      margin: 0;
      padding: 0;
    }

    .container {
      max-width: 600px;
      margin: 50px auto;
      background-color: #fff;
      padding: 20px;
      border-radius: 10px;
      box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
      text-align: center;
    }

    h1 {
      font-size: 24px;
      margin-bottom: 20px;
    }
    .form {
      text-align: left;
    }

    .input-group {
      margin-bottom: 20px;
    }

    .input-group label {
      display: block;
      margin-bottom: 5px;
      font-weight: bold;
    }

    .input-group input {
      width: 100%;
      padding: 10px;
      border-radius: 5px;
      border: 1px solid #ccc;
      box-sizing: border-box;
    }

    .button {
      display: inline-block;
      padding: 10px 20px;
      margin-right: 10px;
      background-color: #4CAF50; /* Dark green button color */
      color: white;
      border: none;
      border-radius: 5px;
      cursor: pointer;
      transition: background-color 0.3s;
    }

    .button:hover {
      background-color: #45a049;
    }
  </style>
</head>
<body>
  <div class="container">
    <?php
    require "sessionauthentication.php";
    require "database.php";
    $token = $_POST['nocsrftoken'];
    if (!isset($token) || $token !== $_SESSION['nocsrftoken']) {
        echo "CSRF Attack is detected";
        die();
    }

    $username = $_SESSION['username'];
    $newPassword = $_POST['newpassword'];
    if (isset($username) && isset($newPassword)) {
        echo "Debug> changepassword.php got username = $username; got password = $newPasswor
        if (changepassword($username, $newPassword)) {
            echo "Password has been changed";
        } else {
            echo "Change password failed!";
        }
    } else {
        echo "No username/password provided!";
    }
    ?>
    <form action="form.php" method="GET">
        <button class="button" type="submit">Go back to login page</button>
    </form>
  </div>
</body>
</html>
```

usermanagement.php

```
<?php
session_start();

require_once "database.php";

// Check if the logged-in user is a superuser
$userProfile = fetchUserProfile($_SESSION['username']);
if ($userProfile && $userProfile['superuser'] != 1) {
    echo "<script>alert('Access denied. Only superusers can access this page.');</script>";
    header("Refresh:0; url=index.php");
    die();
}

// Handle enabling or disabling user accounts
if (isset($_POST['action']) && isset($_POST['username'])) {
    $action = $_POST['action'];
    $username = $_POST['username'];
    if ($action === 'enable') {
        changeUserStatus($username, 1);
        echo "<script>alert('User account enabled.');</script>";
    } elseif ($action === 'disable') {
        changeUserStatus($username, 0);
        echo "<script>alert('User account disabled.');</script>";
    }
}

?>
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Welcome Page</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color: #f0fff0;
    }

    .container {
      text-align: center;
      padding-top: 20px;
    }

    .welcome-text {
      font-size: 24px;
      font-weight: bold;
      margin-bottom: 20px;
    }

    .links {
      display: flex;
      justify-content: center;
      align-items: center;
      flex-wrap: wrap;
    }

    .links form {
      margin: 10px;
    }

    .links button {
      padding: 10px 20px;
      font-size: 16px;
      cursor: pointer;
      background-color: #007bff;
      color: white;
      border: none;
      border-radius: 5px;
      transition: background-color 0.3s;
    }

    .links button:hover {
      background-color: #0056b3;
    }

    .post-container {
      margin-bottom: 20px;
    }

    .post {
      background-color: #f9f9f9;
      border-radius: 8px;
      padding: 20px;
    }

    .post h3 {
      margin-top: 0;
    }

    .post p {
      margin-bottom: 10px;
    }

    .comment {
      background-color: #f0f0f0;
      border-radius: 4px;
      padding: 10px;
      margin-top: 10px;
    }

    .comment p {
      margin-bottom: 5px;
    }

    .add-comment-form {
      margin-top: 10px;
    }
```

```
  .add-comment-form textarea {
    width: calc(100% - 20px);
    padding: 10px;
    border: 1px solid #ccc;
    border-radius: 4px;
    resize: vertical;
    margin-bottom: 10px;
  }

  .add-comment-form input[type="submit"] {
    background-color: #007bff;
    color: white;
    border: none;
    padding: 10px 20px;
    border-radius: 4px;
    cursor: pointer;
    transition: background-color 0.3s;
  }

  .add-comment-form input[type="submit"]:hover {
    background-color: #0056b3;
  }

  /* Adjust home button color */
  button[type="submit"] {
    background-color: #007bff;
    color: white;
    border: none;
    padding: 10px 20px;
    border-radius: 4px;
    cursor: pointer;
    transition: background-color 0.3s;
  }

  button[type="submit"]:hover {
    background-color: #0056b3;
  }

  .edit-delete-container {
    display: inline-block;
  }

  .edit-post-form, .delete-post-form {
    display: inline;
  }
</style>
```

```
</head>
<body>
  <div class="container">
      <?php
      echo "<div class='welcome-text'>Welcome " . htmlentities($_SESSION['username']) . "!</
      ?>
      <div class="links">
        <form id="home" action="index.php" method="POST">
          <button type="submit">Home</button>
        </form>
        <form id="changepasswordform" action="changepasswordform.php" method="POST">
          <input type="hidden" name="username" value="<?php echo urlencode($_SESSION['userna
          <button type="submit">Change Password</button>
        </form>
        <form id="viewprofileform" action="viewprofile.php" method="POST">
          <input type="hidden" name="username" value="<?php echo urlencode($_SESSION['userna
          <button type="submit">View/Edit Profile</button>
        </form>
        <form id="addpostform" action="addpost.php" method="POST">
          <button type="submit">Add Post</button>
        </form>
        <form id="logout" action="logout.php" method="POST">
          <button type="submit">Logout</button>
        </form>
    </div>

    <h1>Users</h1>

    <?php
    // Fetch all users
    $users = $mysqli->query("SELECT * FROM users");

    if ($users->num_rows > 0) {
        while ($row = $users->fetch_assoc()) {
            echo "<div class='user-container'>";
            echo "<p>Username: " . htmlspecialchars($row['username']) . "</p>";
            echo "<p>Fullname: " . htmlspecialchars($row['fullname']) . "</p>";
            echo "<p>Email: " . htmlspecialchars($row['otheremail']) . "</p>";
            echo "<p>Phone: " . htmlspecialchars($row['phone']) . "</p>";
            echo "<p>Status: " . ($row['account_enabled'] == 1 ? "Enabled" : "Disabled") . "

            // Enable/disable user account form
            if ($row['account_enabled'] == 1) {
                echo "<form action='' method='POST'>";
                echo "<input type='hidden' name='action' value='disable'>";
                echo "<input type='hidden' name='username' value='" . $row['username'] . "'>
                echo "<button type='submit'>Disable Account</button>";
                echo "</form>";
            } else {
                echo "<form action='' method='POST'>";
                echo "<input type='hidden' name='action' value='enable'>";
                echo "<input type='hidden' name='username' value='" . $row['username'] . "'
                echo "<button type='submit'>Enable Account</button>";
                echo "</form>";
            }

            echo "</div>";
        }
    } else {
        echo "<p>No users found.</p>";
    }
    ?>
  </div>
</body>
</html>
```

updatepost.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Update Post</title>
  <link rel="stylesheet" href="styles.css">
</head>
<body>
  <div class="container">
    <div class="card">
      <?php
      require "sessionauthentication.php";
      require "database.php";

      if (!isset($_POST['postID']) || !isset($_POST['postContent'])) {
          echo "<h2>Error</h2><p>Post ID or content not provided.</p>";
          die();
      }

      $postID = $_POST['postID'];
      $postContent = htmlspecialchars($_POST['postContent']);
      if (updatePost($postID, $postContent)) {
          echo "<h2>Success</h2><p>Post updated successfully.</p>";
      } else {
          echo "<h2>Error</h2><p>Failed to update post.</p>";
      }

      header("Refresh:2; url=viewposts.php");
      ?>
    </div>
  </div>
</body>
</html>
```

editpost.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Edit Post</title>
  <link rel="stylesheet" href="styles.css">
</head>
<body>
  <div class="container">
    <div class="card">
      <?php
      require "sessionauthentication.php";
      require "database.php";

      if (!isset($_POST['postID'])) {
          echo "<h2>Error</h2><p>Post ID not provided.</p>";
          die();
      }

      $postID = $_POST['postID'];

      $post = $mysqli->query("SELECT postContent FROM posts WHERE postID = $postID")->fetch_

      if (!$post) {
          echo "<h2>Error</h2><p>Post not found.</p>";
          die();
      }
      ?>
      <h2>Edit Post</h2>
      <form action="updatepost.php" method="POST">
```

```
          <input type="hidden" name="postID" value="<?= $postID ?>">
          <div class="input-group">
              <textarea name="postContent" rows="4" cols="50" class="text_field" required><?
          </div>
          <button class="button" type="submit">Update</button>
      </form>
    </div>
  </div>
</body>
</html>
```