**edit\_profile.php**

<?php

session\_start();

include 'db\_connect.php';

if (!isset($\_SESSION['username'])) {

    header('Location: login.php');

    exit;

}

$enrollment = $\_SESSION['enrollment'];

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

    $name = $\_POST['name'];

    $branch = $\_POST['branch'];

    $current\_password = $\_POST['current\_password'];

    $new\_password = !empty($\_POST['new\_password']) ? password\_hash($\_POST['new\_password'], PASSWORD\_DEFAULT) : null;

    $sql = "SELECT password, photo FROM students WHERE enrollment='$enrollment'";

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

    $row = mysqli\_fetch\_assoc($result);

    if (password\_verify($current\_password, $row['password'])) {

        $update\_password\_sql = $new\_password ? ", password='$new\_password'" : "";

        if (!empty($\_FILES['photo']['name'])) {

            $photo = $\_FILES['photo']['name'];

            $photo\_tmp = $\_FILES['photo']['tmp\_name'];

            $photo\_folder = 'uploads/' . $photo;

            if (move\_uploaded\_file($photo\_tmp, $photo\_folder)) {

                $photo\_sql = ", photo='$photo\_folder'";

            } else {

                $\_SESSION['message'] = "Failed to upload photo.";

                header('Location: edit\_profile.php');

                exit;

            }

        } else {

            $photo\_sql = "";

        }

        $update\_sql = "UPDATE students SET name='$name', branch='$branch' $update\_password\_sql $photo\_sql WHERE enrollment='$enrollment'";

        if (mysqli\_query($conn, $update\_sql)) {

            $\_SESSION['message'] = "Profile updated successfully.";

            $\_SESSION['username'] = $name; *// Update the session username*

            header('Location: welcome.php');

            exit;

        } else {

            $\_SESSION['message'] = "Error updating profile: " . mysqli\_error($conn);

        }

    } else {

        $\_SESSION['message'] = "Current password is incorrect.";

    }

}

?>

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

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

    <title>Edit Profile</title>

    <link rel="stylesheet" href="styles.css">

</head>

<body>

    <div class="container">

        <h2>Edit Profile</h2>

        <?php

        if (isset($\_SESSION['message'])) {

            echo "<p class='error'>" . $\_SESSION['message'] . "</p>";

            unset($\_SESSION['message']);

        }

        ?>

        <form action="edit\_profile.php" method="POST" enctype="multipart/form-data">

            <label>Name: </label>

            <input type="text" name="name" value="<?php echo htmlspecialchars($\_SESSION['username']); ?>" required>

            <label>Branch: </label>

            <select name="branch" required>

                <option value="IT" <?php echo isset($\_SESSION['branch']) && $\_SESSION['branch'] == 'IT' ? 'selected' : ''; ?>>IT</option>

                <option value="CE" <?php echo isset($\_SESSION['branch']) && $\_SESSION['branch'] == 'CE' ? 'selected' : ''; ?>>CE</option>

                <option value="IOT" <?php echo isset($\_SESSION['branch']) && $\_SESSION['branch'] == 'IOT' ? 'selected' : ''; ?>>IOT</option>

                <option value="ME" <?php echo isset($\_SESSION['branch']) && $\_SESSION['branch'] == 'ME' ? 'selected' : ''; ?>>ME</option>

                <option value="EE" <?php echo isset($\_SESSION['branch']) && $\_SESSION['branch'] == 'EE' ? 'selected' : ''; ?>>EE</option>

            </select>

            <label>Current Password: </label>

            <input type="password" name="current\_password" required>

            <label>New Password (leave blank to keep current password): </label>

            <input type="password" name="new\_password">

            <label>Photo: </label>

            <input type="file" name="photo">

            <input type="submit" value="Update Profile">

        </form>

        <a href="welcome.php">Go back</a>

    </div>

</body>

</html>

**Welcome.php**

<?php

session\_start();

include 'db\_connect.php';

if (!isset($\_SESSION['username'])) {

    header('Location: login.php');

    exit;

}

$enrollment = $\_SESSION['enrollment'];

$sql = "SELECT photo FROM students WHERE enrollment='$enrollment'";

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

$row = mysqli\_fetch\_assoc($result);

$photo = $row['photo'];

?>

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

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

    <title>Welcome</title>

    <link rel="stylesheet" href="styles.css">

</head>

<body>

    <div class="container">

        <h2>Welcome, <?php echo htmlspecialchars($\_SESSION['username']); ?>!</h2>

        <p>Enrollment: <?php echo htmlspecialchars($\_SESSION['enrollment']); ?></p>

        <div class="profile-picture">

            <img src="<?php echo htmlspecialchars($photo); ?>" alt="Profile Picture"> </div>

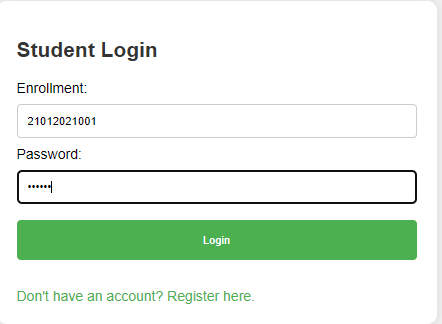
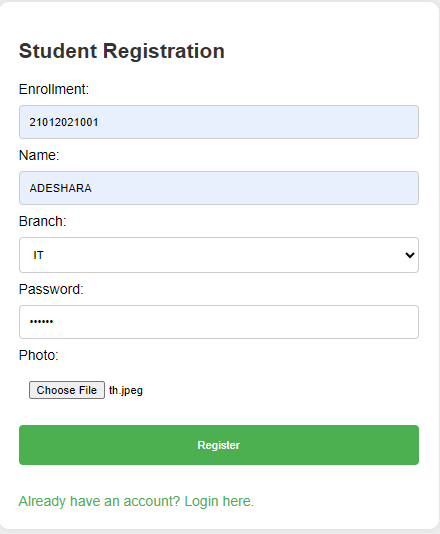
        <p><a href="edit\_profile.php">Edit Profile</a></p>

        <p><a href="logout.php">Logout</a></p>

    </div>

</body>

</html>

****

