## 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');
```

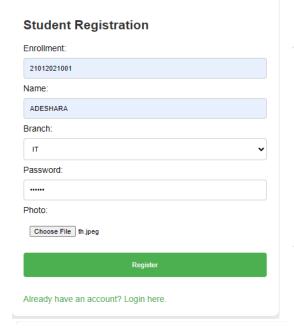
```
exit:
    } else {
      $_SESSION['message'] = "Error updating profile: " . mysqli_error($conn);
    }
  } else {
    $_SESSION['message'] = "Current password is incorrect.";
  }
?>
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Edit Profile</title>
  k rel="stylesheet" href="styles.css">
</head>
<body>
  <div class="container">
    <h2>Edit Profile</h2>
    <?php
    if (isset($ SESSION['message'])) {
      echo "" . $_SESSION['message'] . "";
      unset($_SESSION['message']);
    }
    <form action="edit_profile.php" method="POST" enctype="multipart/form-data">
      <label>Name: </label>
      <input type="text" name="name" value="<?php echo</pre>
htmlspecialchars($_SESSION['username']); ?>" required>
      <label>Branch: </label>
      <select name="branch" required>
         <option value="IT" <?php echo isset($_SESSION['branch']) &&</pre>
$_SESSION['branch'] == 'IT' ? 'selected' : "; ?>>IT</option>
         <option value="CE" <?php echo isset($_SESSION['branch']) &&</pre>
$_SESSION['branch'] == 'CE' ? 'selected' : "; ?>>CE</option>
         <option value="IOT" <?php echo isset($_SESSION['branch']) &&</pre>
$_SESSION['branch'] == 'IOT' ? 'selected' : "; ?>>IOT</option>
         <option value="ME" <?php echo isset($_SESSION['branch']) &&</pre>
$_SESSION['branch'] == 'ME' ? 'selected' : "; ?>>ME</option>
         <option value="EE" <?php echo isset($ SESSION['branch']) &&</pre>
$_SESSION['branch'] == 'EE' ? 'selected' : "; ?>>EE</option>
```

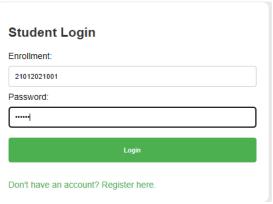
```
</select>
<label>Current Password: </label>
<input type="password" name="current_password" required>
<label>New Password (leave blank to keep current password): </label>
<input type="password" name="new_password">
<label>Photo: </label>
<input type="file" name="photo">
<input type="file" name="photo">
<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 = $row['photo'];
?>
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Welcome</title>
  k rel="stylesheet" href="styles.css">
</head>
<body>
  <div class="container">
    <h2>Welcome, <?php echo htmlspecialchars($_SESSION['username']); ?>!</h2>
    Enrollment: <?php echo htmlspecialchars($_SESSION['enrollment']); ?>
```

<div class="profile-picture"></div>
<img alt="Profile Picture" src="&lt;?php echo htmlspecialchars(\$photo); ?&gt;"/>
<a href="edit_profile.php">Edit Profile</a>
<a href="logout.php">Logout</a>





## **Edit Profile**

