**Practical – 8**

**Aim: Perform following programs of PHP with database.**

**Exercise:**

1. **Create Login module for Student with registration page, login page, welcome page, change password page and logout page. [Note: Student’s registration fields Enrollment, Name, Branch, Password, Photo].**

**Register.php**

<?php

session\_start();

include 'db\_connect.php';

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

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

    $name = $\_POST['name'];

    $branch = $\_POST['branch'];

    $password = password\_hash($\_POST['password'], PASSWORD\_DEFAULT);

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

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

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

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

        $sql = "INSERT INTO students (enrollment, name, branch, password, photo) VALUES ('$enrollment', '$name', '$branch', '$password', '$photo\_folder')";

        if (mysqli\_query($conn, $sql)) {

            $\_SESSION['message'] = "Registration successful!";

            header('Location: login.php');

        } else {

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

        }

    } else {

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

    }

}

?>

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

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

    <title>Student Registration</title>

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

</head>

<body>

    <div class="container">

        <h2>Student Registration</h2>

        <?php

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

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

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

        }

        ?>

        <form action="register.php" method="POST" enctype="multipart/form-data">

            <label>Enrollment: </label>

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

            <label>Name: </label>

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

            <label>Branch: </label>

            <select name="branch" required>

                <option value="IT">IT</option>

                <option value="CE">CE</option>

                <option value="IOT">IOT</option>

                <option value="ME">ME</option>

                <option value="EE">EE</option>

            </select>

            <label>Password: </label>

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

            <label>Photo: </label>

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

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

        </form>

        <a href="login.php">Already have an account? Login here.</a>

    </div>

</body>

</html>

**Login.php**

<?php

session\_start();

include 'db\_connect.php';

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

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

    $password = $\_POST['password'];

    $sql = "SELECT \* FROM students WHERE enrollment='$enrollment'";

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

    if (mysqli\_num\_rows($result) == 1) {

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

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

            $\_SESSION['username'] = $row['name'];

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

            header('Location: welcome.php');

        } else {

            $\_SESSION['message'] = "Invalid password.";

        }

    } else {

        $\_SESSION['message'] = "Invalid enrollment number.";

    }

}

?>

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

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

    <title>Student Login</title>

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

</head>

<body>

    <div class="container">

        <h2>Student Login</h2>

        <?php

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

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

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

        }

        ?>

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

            <label>Enrollment: </label>

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

            <label>Password: </label>

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

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

        </form>

        <a href="register.php">Don't have an account? Register here.</a>

    </div>

</body>

</html>

**Logout.php**

<?php

session\_start();

session\_destroy();

header('Location: login.php');

exit;

?>

**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>

**Db\_connect.php**

<?php

$servername = "localhost";

$username = "root";

$password = "";

$dbname = "WT\_P7";

*// Create connection*

$conn = mysqli\_connect($servername, $username, $password, $dbname);

*// Check connection*

if (!$conn) {

    die("Connection failed: " . mysqli\_connect\_error());

}

?>

**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>

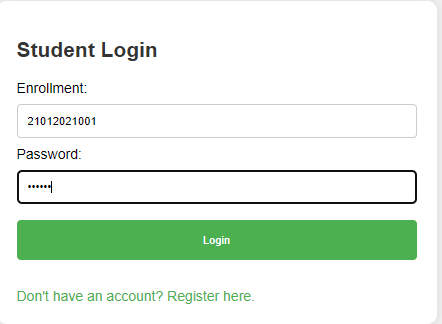
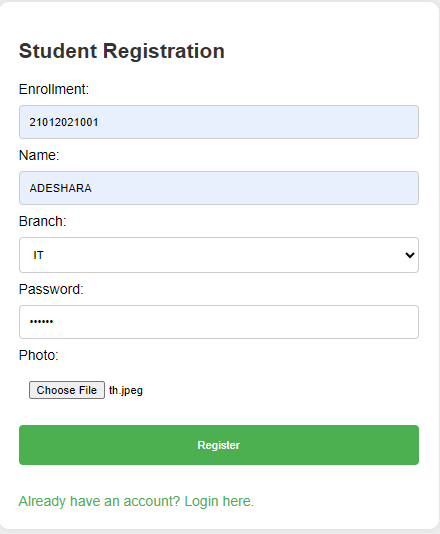
        <p><a href="edit\_profile.php">Edit Profile</a></p>

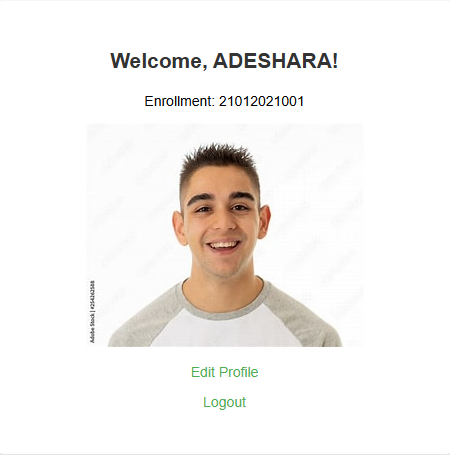
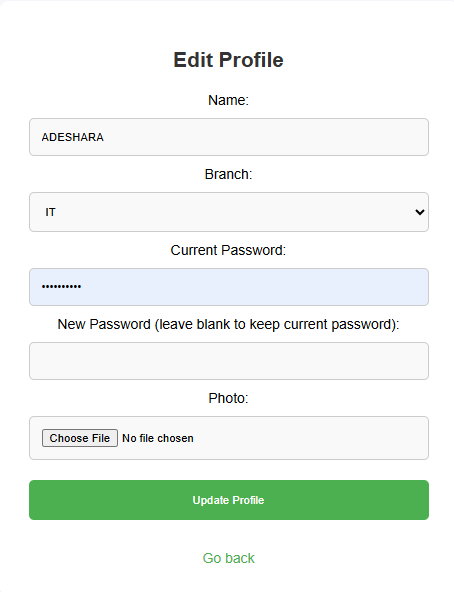
        <p><a href="logout.php">Logout</a></p>

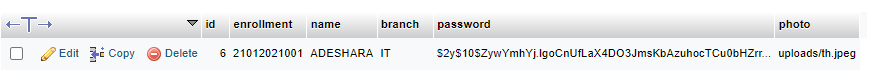
    </div>

</body>

</html>

****





1. **Create Admin module to perform update, delete, display records with order by and search operation with Student table. [Note: Same as grid view design].**

**Admin\_login.php**

<?php

session\_start();

include 'db\_connect.php';

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

$username = $\_POST['username'];

$password = $\_POST['password'];

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

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

if (mysqli\_num\_rows($result) == 1) {

$\_SESSION['admin'] = $username;

header('Location: admin\_dashboard.php');

} else {

$\_SESSION['message'] = "Invalid username or password.";

}

}

?>

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

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

<title>Admin Login</title>

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

</head>

<body>

<div class="container">

<h2>Admin Login</h2>

<?php

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

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

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

}

?>

<form action="admin\_login.php" method="POST">

<label>Username: </label>

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

<label>Password: </label>

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

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

</form>

</div>

</body>

</html>

**Admin\_dashboard.php**

<?php

session\_start();

include 'db\_connect.php';

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

    header('Location: admin\_login.php');

    exit;

}

$search = '';

if (isset($\_GET['search'])) {

    $search = $\_GET['search'];

    $sql = "SELECT \* FROM students WHERE name LIKE '%$search%' ORDER BY name";

} else {

    $sql = "SELECT \* FROM students ORDER BY name";

}

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

?>

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

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

    <title>Admin Dashboard</title>

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

</head>

<body>

    <div class="container">

        <h2>Admin Dashboard</h2>

        <form action="admin\_dashboard.php" method="GET">

            <input type="text" name="search" placeholder="Search by name" value="<?php echo $search; ?>">

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

        </form>

        <table>

            <thead>

                <tr>

                    <th>Enrollment</th>

                    <th>Name</th>

                    <th>Branch</th>

                    <th>Actions</th>

                </tr>

            </thead>

            <tbody>

                <?php while ($row = mysqli\_fetch\_assoc($result)) { ?>

                <tr>

                    <td><?php echo $row['enrollment']; ?></td>

                    <td><?php echo $row['name']; ?></td>

                    <td><?php echo $row['branch']; ?></td>

                    <td>

                        <a href="update\_student.php?id=<?php echo $row['id']; ?>">Update</a>

                        <a href="delete\_student.php?id=<?php echo $row['id']; ?>" onclick="return confirm('Are you sure you want to delete this record?')">Delete</a>

                    </td>

                </tr>

                <?php } ?>

            </tbody>

        </table>

        <a href="admin\_logout.php">Logout</a>

    </div>

</body>

</html>

**Update\_student.php**

<?php

session\_start();

include 'db\_connect.php';

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

    header('Location: admin\_login.php');

    exit;

}

if (isset($\_GET['id'])) {

    $id = $\_GET['id'];

    $sql = "SELECT \* FROM students WHERE id='$id'";

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

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

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

        $name = $\_POST['name'];

        $branch = $\_POST['branch'];

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

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

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

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

            header('Location: admin\_dashboard.php');

        } else {

            $\_SESSION['message'] = "Error updating record.";

        }

    }

} else {

    header('Location: admin\_dashboard.php');

}

?>

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

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

    <title>Update Student</title>

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

</head>

<body>

    <div class="container">

        <h2>Update Student</h2>

        <?php

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

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

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

        }

        ?>

        <form action="update\_student.php?id=<?php echo $id; ?>" method="POST">

            <label>Name: </label>

            <input type="text" name="name" value="<?php echo $student['name']; ?>" required>

            <label>Branch: </label>

            <select name="branch" required>

                <option value="IT" <?php echo $student['branch'] == 'IT' ? 'selected' : ''; ?>>IT</option>

                <option value="CE" <?php echo $student['branch'] == 'CE' ? 'selected' : ''; ?>>CE</option>

                <option value="IOT" <?php echo $student['branch'] == 'IOT' ? 'selected' : ''; ?>>IOT</option>

            </select>

            <label>Enrollment: </label>

            <input type="text" name="enrollment" value="<?php echo $student['enrollment']; ?>" required>

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

        </form>

        <a href="admin\_dashboard.php">Go back</a>

    </div>

</body>

</html>

**Delete\_student.php**

<?php

session\_start();

include 'db\_connect.php';

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

    header('Location: admin\_login.php');

    exit;

}

if (isset($\_GET['id'])) {

    $id = $\_GET['id'];

    $delete\_sql = "DELETE FROM students WHERE id='$id'";

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

        $\_SESSION['message'] = "Record deleted successfully.";

    } else {

        $\_SESSION['message'] = "Error deleting record.";

    }

}

header('Location: admin\_dashboard.php');

?>

**Db\_connect.php**

<?php

$servername = "localhost";

$username = "root";

$password = "";

$dbname = "WT\_P7";

*// Create connection*

$conn = mysqli\_connect($servername, $username, $password, $dbname);

*// Check connection*

if (!$conn) {

    die("Connection failed: " . mysqli\_connect\_error());

}

?>

**Admin\_logout.php**

<?php

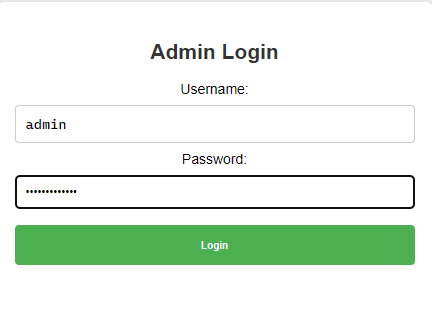
session\_start();

session\_destroy();

header('Location: admin\_login.php');

exit;

?>

****

