GANPAT UNIVERSITY
U.V. PATEL COLLEGE OF ENGINEERING

B.Tech 6th Semester CE/IT
2CEIT6PE1: Web Technology

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]

Code:

Config.php

```php
<?php
session_start();
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "student_login_system";

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

if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

function hashPassword($password) {
    return password_hash($password, PASSWORD_DEFAULT);
}

function verifyPassword($password, $hash) {
    return password_verify($password, $hash);
}
?>
```

register.php:

```php
<?php
include 'config.php';
```

```php
if ($_SERVER["REQUEST_METHOD"] == "POST") {
    $enrollment = $_POST['enrollment'];
    $name = $_POST['name'];
    $branch = $_POST['branch'];
    $password = hashPassword($_POST['password']);
    $photo = $_FILES['photo']['name'];
    $target = "uploads/" . basename($photo);

    if (move_uploaded_file($_FILES['photo']['tmp_name'], $target)) {
        $sql = "INSERT INTO students (enrollment, name, branch, password, photo) VALUES
('$enrollment', '$name', '$branch', '$password', '$target')";
        if ($conn->query($sql) === TRUE) {
            $_SESSION['message'] = "Registration successful! Please log in.";
            header('Location: login.php');
        } else {
            $_SESSION['error'] = "Error: " . $sql . "<br>" . $conn->error;
        }
    } else {
        $_SESSION['error'] = "Failed to upload photo.";
    }
}
?>


<?php include 'templates/header.php'; ?>
<div class="container mt-5">
    <h2 class="text-center">Register</h2>
    <div class="card">
        <div class="card-body">
            <form method="POST" enctype="multipart/form-data" class="mt-4">
                <div class="mb-3">
                    <label for="enrollment" class="form-label">Enrollment</label>
                    <input type="text" class="form-control" id="enrollment" name="enrollment"
required>
                </div>
                <div class="mb-3">
                    <label for="name" class="form-label">Name</label>
                    <input type="text" class="form-control" id="name" name="name" required>
                </div>
                <div class="mb-3">
                    <label for="branch" class="form-label">Branch</label>
                    <input type="text" class="form-control" id="branch" name="branch" required>
                </div>
                <div class="mb-3">
                    <label for="password" class="form-label">Password</label>
                    <input type="password" class="form-control" id="password" name="password"
required>
                </div>
                <div class="mb-3">
                    <label for="photo" class="form-label">Photo</label>
                    <input type="file" class="form-control" id="photo" name="photo" required>
```

```
            </div>
            <button type="submit" class="btn btn-primary btn-block">Register</button>
        </form>
      </div>
    </div>
</div>
<?php include 'templates/footer.php'; ?>
```

Login.php:

```php
<?php
include 'config.php';

if ($_SERVER["REQUEST_METHOD"] == "POST") {
   $enrollment = $_POST['enrollment'];
   $password = $_POST['password'];

   $sql = "SELECT * FROM students WHERE enrollment = '$enrollment'";
   $result = $conn->query($sql);

   if ($result->num_rows == 1) {
      $student = $result->fetch_assoc();
      if (verifyPassword($password, $student['password'])) {
         $_SESSION['student_id'] = $student['id'];
         $_SESSION['enrollment'] = $student['enrollment'];
         $_SESSION['name'] = $student['name'];
         $_SESSION['photo'] = $student['photo'];
         header('Location: welcome.php');
      } else {
         $_SESSION['error'] = "Invalid password.";
      }
   } else {
      $_SESSION['error'] = "Invalid enrollment number.";
   }
}
?>

<?php include 'templates/header.php'; ?>
<div class="container mt-5">
   <h2 class="text-center">Login</h2>
   <div class="card">
      <div class="card-body">
         <form method="POST" class="mt-4">
            <div class="mb-3">
               <label for="enrollment" class="form-label">Enrollment</label>
               <input type="text" class="form-control" id="enrollment" name="enrollment"
required>
            </div>
            <div class="mb-3">
               <label for="password" class="form-label">Password</label>
```

```
            <input type="password" class="form-control" id="password" name="password"
required>
          </div>
          <button type="submit" class="btn btn-primary btn-block">Login</button>
        </form>
      </div>
    </div>
</div>
<?php include 'templates/footer.php'; ?>
```

Logout.php:

```
<?php
session_start();
session_unset();
session_destroy();
header('Location: login.php');
?>
```

Welcome.php:

```
<?php
include 'config.php';
if (!isset($_SESSION['student_id'])) {
    header('Location: login.php');
    exit;
}
?>

<?php include 'templates/header.php'; ?>
<div class="container mt-5 text-center">
    <h2>Welcome, <?php echo $_SESSION['name']; ?>!</h2>
    <img src="<?php echo $_SESSION['photo']; ?>" alt="Profile Photo" class="img-
thumbnail rounded-circle img-center">
    <p>This is the welcome page.</p>
    <div class="welcome-buttons mt-3">
      <a href="change_password.php" class="btn btn-secondary">Change Password</a>
      <a href="logout.php" class="btn btn-danger">Logout</a>
    </div>
</div>
<?php include 'templates/footer.php'; ?>
```

Change_password.php:

```
<?php
include 'config.php';

if (!isset($_SESSION['student_id'])) {
    header('Location: login.php');
    exit;
```

```php
}

if ($_SERVER["REQUEST_METHOD"] == "POST") {
    $current_password = $_POST['current_password'];
    $new_password = $_POST['new_password'];

    $student_id = $_SESSION['student_id'];
    $sql = "SELECT password FROM students WHERE id = '$student_id'";
    $result = $conn->query($sql);
    $student = $result->fetch_assoc();

    if (verifyPassword($current_password, $student['password'])) {
        $new_password_hashed = hashPassword($new_password);
        $sql = "UPDATE students SET password = '$new_password_hashed' WHERE id =
'$student_id'";
        if ($conn->query($sql) === TRUE) {
            $_SESSION['message'] = "Password changed successfully!";
        } else {
            $_SESSION['error'] = "Error updating password: " . $conn->error;
        }
    } else {
        $_SESSION['error'] = "Current password is incorrect.";
    }
}
?>


<?php include 'templates/header.php'; ?>
<div class="container mt-5">
    <h2 class="text-center">Change Password</h2>
    <div class="card">
        <div class="card-body">
            <form method="POST" class="mt-4">
                <div class="mb-3">
                    <label for="current_password" class="form-label">Current Password</label>
                    <input type="password" class="form-control" id="current_password"
name="current_password" required>
                </div>
                <div class="mb-3">
                    <label for="new_password" class="form-label">New Password</label>
                    <input type="password" class="form-control" id="new_password"
name="new_password" required>
                </div>
                <button type="submit" class="btn btn-primary btn-block">Change
Password</button>
            </form>
        </div>
    </div>
</div>
<?php include 'templates/footer.php'; ?>
```

Header.php:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Student Login System</title>
    <!-- <link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/5.1.3/css/bootstrap.min.css"> -->
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css"
rel="stylesheet" integrity="sha384-
QWTKZyjpPEjISv5WaRU9OFeRpok6YctnYmDr5pNlyT2bRjXh0JMhjY6hW+ALEwIH"
crossorigin="anonymous">
    <link rel="stylesheet" href="../static/css/styles.css">
</head>
<body>
<nav class="navbar navbar-expand-lg navbar-light bg-light">
    <div class="container-fluid">
        <a class="navbar-brand" href="#">Student Login System</a>
        <button class="navbar-toggler" type="button" data-bs-toggle="collapse" data-bs-
target="#navbarNav" aria-controls="navbarNav" aria-expanded="false" aria-label="Toggle
navigation">
            <span class="navbar-toggler-icon"></span>
        </button>
        <div class="collapse navbar-collapse justify-content-center" id="navbarNav">
            <ul class="navbar-nav">
                <li class="nav-item"><a class="nav-link"
href="../welcome.php">Welcome</a></li>
                <li class="nav-item"><a class="nav-link" href="../change_password.php">Change
Password</a></li>
                <li class="nav-item"><a class="nav-link" href="../logout.php">Logout</a></li>
                <li class="nav-item"><a class="nav-link" href="index.php">Admin Panel</a></li>
            </ul>
        </div>
    </div>
</nav>
<div class="container mt-4">
    <?php if (isset($_SESSION['message'])): ?>
        <div class="alert alert-success"><?php echo $_SESSION['message'];
unset($_SESSION['message']); ?></div>
    <?php endif; ?>
    <?php if (isset($_SESSION['error'])): ?>
        <div class="alert alert-danger"><?php echo $_SESSION['error'];
unset($_SESSION['error']); ?></div>
    <?php endif; ?>
```

Footer.php:

```
</div>
```

```
<script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"
integrity="sha384-
YvpcrYf0tY3lHB60NNkmXc5s9fDVZLESaAA55NDzOxhy9GkcIdslK1eN7N6jIeHz"
crossorigin="anonymous"></script>
<script
src="https://cdn.jsdelivr.net/npm/@popperjs/core@2.10.2/dist/umd/popper.min.js"></script>
<script
src="https://stackpath.bootstrapcdn.com/bootstrap/5.1.3/js/bootstrap.min.js"></script>
<script src="../static/js/scripts.js"></script>
</body>
</html>
```
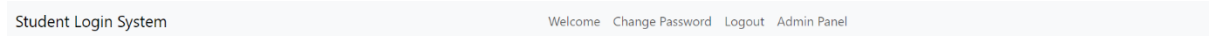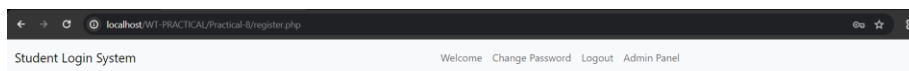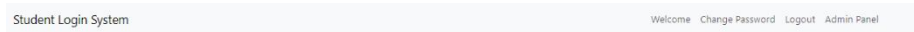
Output:

Exercise-2:

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

Code:

Config.php:

```php
<?php
session_start();
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "student_login_system";

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

if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

function hashPassword($password) {
    return password_hash($password, PASSWORD_DEFAULT);
}

function verifyPassword($password, $hash) {
    return password_verify($password, $hash);
}
?>
```

Index.php:
```php
<?php
```

```php
include 'config.php';

$order = $_GET['order'] ?? 'name';
$search = $_GET['search'] ?? '';

$sql = "SELECT * FROM students WHERE name LIKE '%$search%' OR enrollment LIKE '%$search%' ORDER BY $order";
$result = $conn->query($sql);
?>
```

```php
<?php include '../templates/header.php'; ?>
<div class="container mt-5">
    <h2 class="text-center">Student Records</h2>
    <div class="text-center mb-4">
        <form method="GET" class="form-inline justify-content-center">
            <input type="text" class="form-control mr-2" name="search" placeholder="Search by name or enrollment" value="<?php echo $search; ?>">
            <button type="submit" class="btn btn-primary">Search</button>
        </form>
    </div>
    <table class="table table-bordered table-striped">
        <thead>
            <tr>
                <th><a href="?order=enrollment">Enrollment</a></th>
                <th><a href="?order=name">Name</a></th>
                <th><a href="?order=branch">Branch</a></th>
                <th>Photo</th>
                <th>Actions</th>
            </tr>
        </thead>
        <tbody>
            <?php while($row = $result->fetch_assoc()): ?>
                <tr>
                    <td><?php echo $row['enrollment']; ?></td>
                    <td><?php echo $row['name']; ?></td>
                    <td><?php echo $row['branch']; ?></td>
                    <td><img src="../<?php echo $row['photo']; ?>" alt="Profile Photo" class="img-thumbnail" width="100"></td>
                    <td>
                        <a href="update.php?id=<?php echo $row['id']; ?>" class="btn btn-warning">Edit</a>
                        <a href="delete.php?id=<?php echo $row['id']; ?>" class="btn btn-danger" onclick="return confirm('Are you sure you want to delete this record?');">Delete</a>
                    </td>
                </tr>
            <?php endwhile; ?>
        </tbody>
    </table>
</div>
<?php include '../templates/footer.php'; ?>
```

Update.php:

```php
<?php
include 'config.php';

if ($_SERVER["REQUEST_METHOD"] == "POST") {
    $id = $_POST['id'];
    $enrollment = $_POST['enrollment'];
    $name = $_POST['name'];
    $branch = $_POST['branch'];
    $photo = $_FILES['photo']['name'];
    $target = "../uploads/" . basename($photo);

    if ($photo) {
        move_uploaded_file($_FILES['photo']['tmp_name'], $target);
        $sql = "UPDATE students SET enrollment='$enrollment', name='$name',
branch='$branch', photo='$target' WHERE id='$id'";
    } else {
        $sql = "UPDATE students SET enrollment='$enrollment', name='$name',
branch='$branch' WHERE id='$id'";
    }

    if ($conn->query($sql) === TRUE) {
        $_SESSION['message'] = "Record updated successfully!";
        header('Location: index.php');
    } else {
        $_SESSION['error'] = "Error updating record: " . $conn->error;
    }
} else {
    $id = $_GET['id'];
    $sql = "SELECT * FROM students WHERE id='$id'";
    $result = $conn->query($sql);
    $student = $result->fetch_assoc();
}
?>

<?php include '../templates/header.php'; ?>
<div class="container mt-5">
    <h2 class="text-center">Update Student Record</h2>
    <div class="card">
        <div class="card-body">
            <form method="POST" enctype="multipart/form-data" class="mt-4">
                <input type="hidden" name="id" value="<?php echo $student['id']; ?>">
                <div class="mb-3">
                    <label for="enrollment" class="form-label">Enrollment</label>
                    <input type="text" class="form-control" id="enrollment" name="enrollment"
value="<?php echo $student['enrollment']; ?>" required>
                </div>
                <div class="mb-3">
                    <label for="name" class="form-label">Name</label>
```

```
        <input type="text" class="form-control" id="name" name="name" value="<?php
echo $student['name']; ?>" required>
        </div>
        <div class="mb-3">
          <label for="branch" class="form-label">Branch</label>
          <input type="text" class="form-control" id="branch" name="branch"
value="<?php echo $student['branch']; ?>" required>
        </div>
        <div class="mb-3">
          <label for="photo" class="form-label">Photo</label>
          <input type="file" class="custom-file-input" id="photo" name="photo">
          <label class="custom-file-label" for="photo">Choose file</label>
        </div>
        <button type="submit" class="btn btn-primary btn-block">Update</button>
      </form>
    </div>
  </div>
</div>
<?php include '../templates/footer.php'; ?>
```

Delete.php:

```
<?php
include 'config.php';

$id = $_GET['id'];
$sql = "DELETE FROM students WHERE id='$id'";

if ($conn->query($sql) === TRUE) {
   $_SESSION['message'] = "Record deleted successfully!";
} else {
   $_SESSION['error'] = "Error deleting record: " . $conn->error;
}

header('Location: index.php');
?>
```

Search.php:

```
<?php
include 'config.php';

$search = $_GET['search'] ?? '';

$sql = "SELECT * FROM students WHERE name LIKE '%$search%' OR enrollment LIKE
'%$search%' ORDER BY name";
$result = $conn->query($sql);

include 'index.php';
?>
```

Output: