**LAB-9**

**K201052**

1. **M.HASSAN ALI**

**Q1.**

<?php

include\_once("config.php");

if (isset($\_POST['submit'])) {

    $name = $\_POST['name'];

    $email = $\_POST['email'];

    $phone = $\_POST['phone'];

    $sql = "INSERT INTO users (name, email, phone) VALUES ('$name', '$email', '$phone')";

    if (mysqli\_query($conn, $sql)) {

        echo "New user created successfully";

        $sql = "SELECT \* FROM users";

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

        if (mysqli\_num\_rows($result) > 0) {

            while ($row = mysqli\_fetch\_assoc($result)) {

                echo "ID: " . $row["id"] . "<br>";

                echo "Name: " . $row["name"] . "<br>";

                echo "Email: " . $row["email"] . "<br>";

                echo "Phone: " . $row["phone"] . "<br>";

                echo "<br>";

            }

            $id = 1;

            $name = 'Hassan';

            $sql = "UPDATE users SET name='$name' WHERE id='$id'";

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

                echo "User updated successfully";

            } else {

                echo "Error: " . $sql . "<br>" . mysqli\_error($conn);

            }

        } else {

            echo "0 results";

        }

    } else {

        echo "Error: " . $sql . "<br>" . mysqli\_error($conn);

    }

}

?>

<form method="post">

    Name: <input type="text" name="name"><br>

    Email: <input type="text" name="email"><br>

    Phone: <input type="text" name="phone"><br>

    <input type="submit" name="submit" value="Submit">

</form>

<?php

$id = 1;

$sql = "DELETE FROM users WHERE id='$id'";

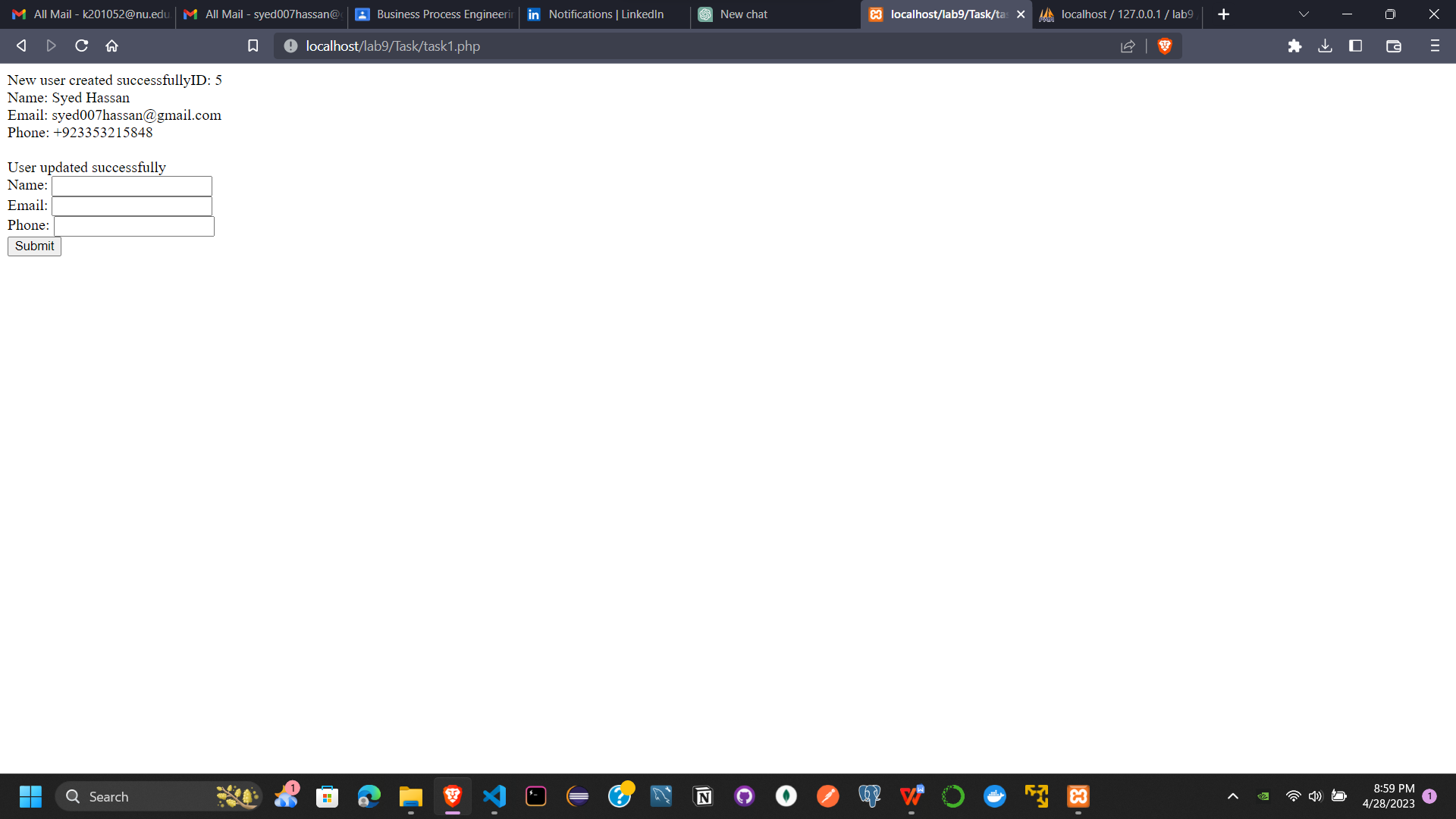
if (mysqli\_query($conn, $sql)) {

    echo "User deleted successfully";

} else {

    echo "Error deleting user: " . mysqli\_error($conn);

}





Q2.

<?php

include\_once("config.php");

session\_start();

if (isset($\_POST['submit'])) {

    $username = $\_POST['username'];

    $password = $\_POST['password'];

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

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

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

        // Login successful

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

        header("Location: task2\_dashboard.php");

        exit();

    } else {

        // Login failed

        $error = "Invalid username or password";

    }

    mysqli\_close($conn);

}

?>

<!DOCTYPE html>

<html>

<head>

    <title>Login</title>

</head>

<body>

    <?php if (isset($error)) { echo $error . "<br>"; } ?>

    <form method="post">

        Username: <input type="text" name="username"><br>

        Password: <input type="password" name="password"><br>

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

    </form>

</body>

</html>

<?php

session\_start();

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

    header("Location: task2\_login.php");

    exit();

}

// CRUD operations go here

?>

<!DOCTYPE html>

<html>

<head>

    <title>Dashboard</title>

</head>

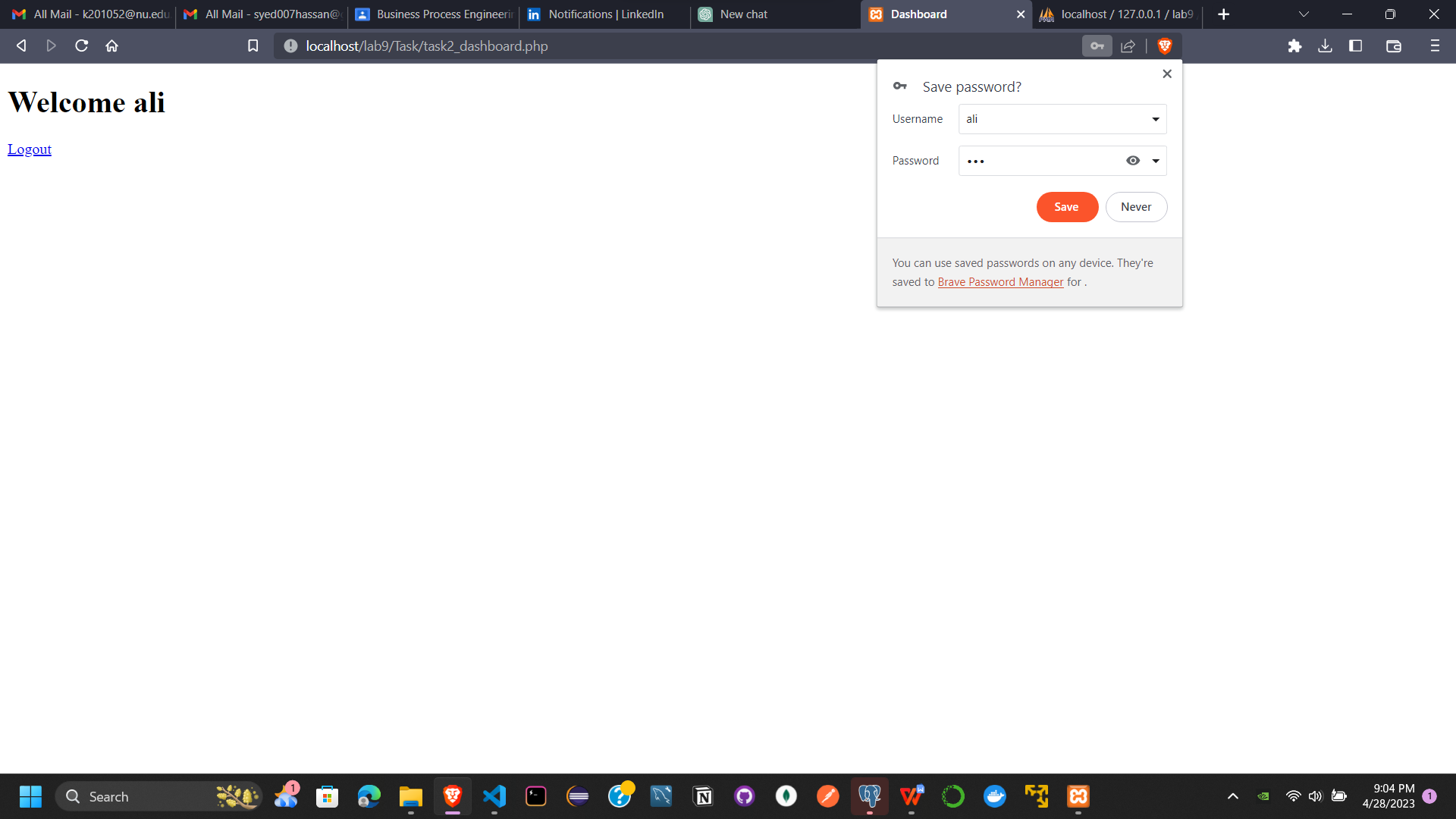
<body>

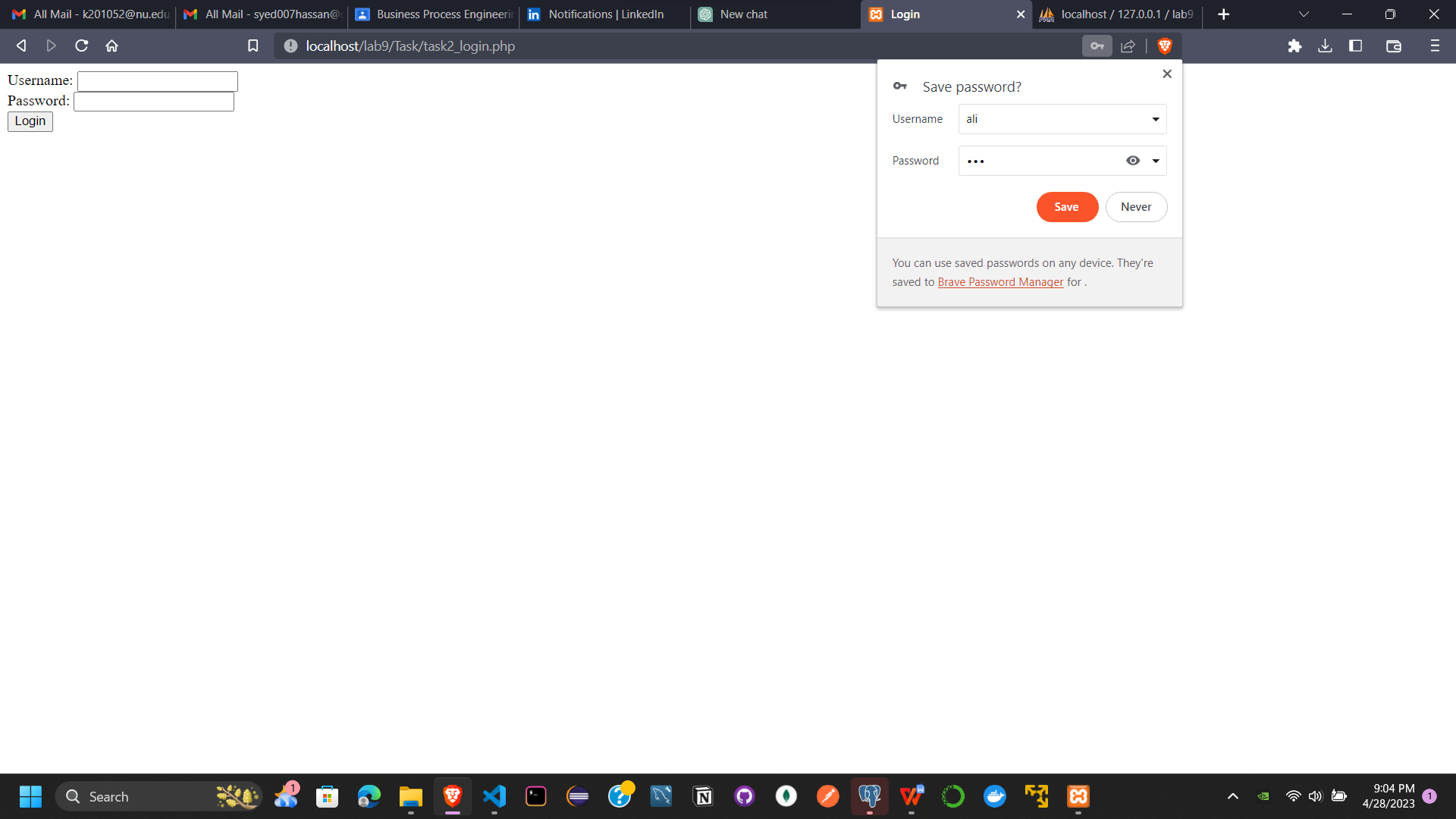
    <h1>Welcome <?php echo $\_SESSION['username']; ?></h1>

    <a href="task2\_logout.php">Logout</a>

</body>

</html>





Q3.

<?php

include\_once("config.php");

if (isset($\_POST['submit'])) {

    $name = $\_POST['name'];

    $email = $\_POST['email'];

    $password = $\_POST['password'];

    // Validate inputs

    if (empty($name) || empty($email) || empty($password)) {

        $error = "Please fill in all fields";

    } elseif (!filter\_var($email, FILTER\_VALIDATE\_EMAIL)) {

        $error = "Invalid email format";

    } else {

        // Check if email already exists in database

        $sql = "SELECT \* FROM users WHERE email='$email'";

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

        if (mysqli\_num\_rows($result) > 0) {

            $error = "Email already exists";

        } else {

            // Insert user into database

            $sql = "INSERT INTO users (name, email, password) VALUES ('$name', '$email', '$password')";

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

                $message = "User created successfully";

            } else {

                $error = "Error creating user: " . mysqli\_error($conn);

            }

        }

    }

    mysqli\_close($conn);

}

?>

<!DOCTYPE html>

<html>

<head>

    <title>Registration</title>

</head>

<body>

    <?php if (isset($error)) { echo $error . "<br>"; } ?>

    <?php if (isset($message)) { echo $message . "<br>"; } ?>

    <form method="post">

        Name: <input type="text" name="name"><br>

        Email: <input type="text" name="email"><br>

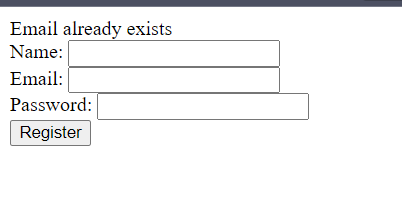
        Password: <input type="password" name="password"><br>

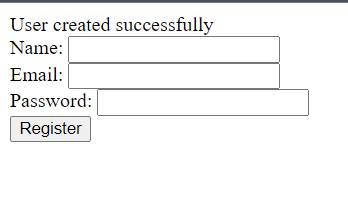
        <input type="submit" name="submit" value="Register">

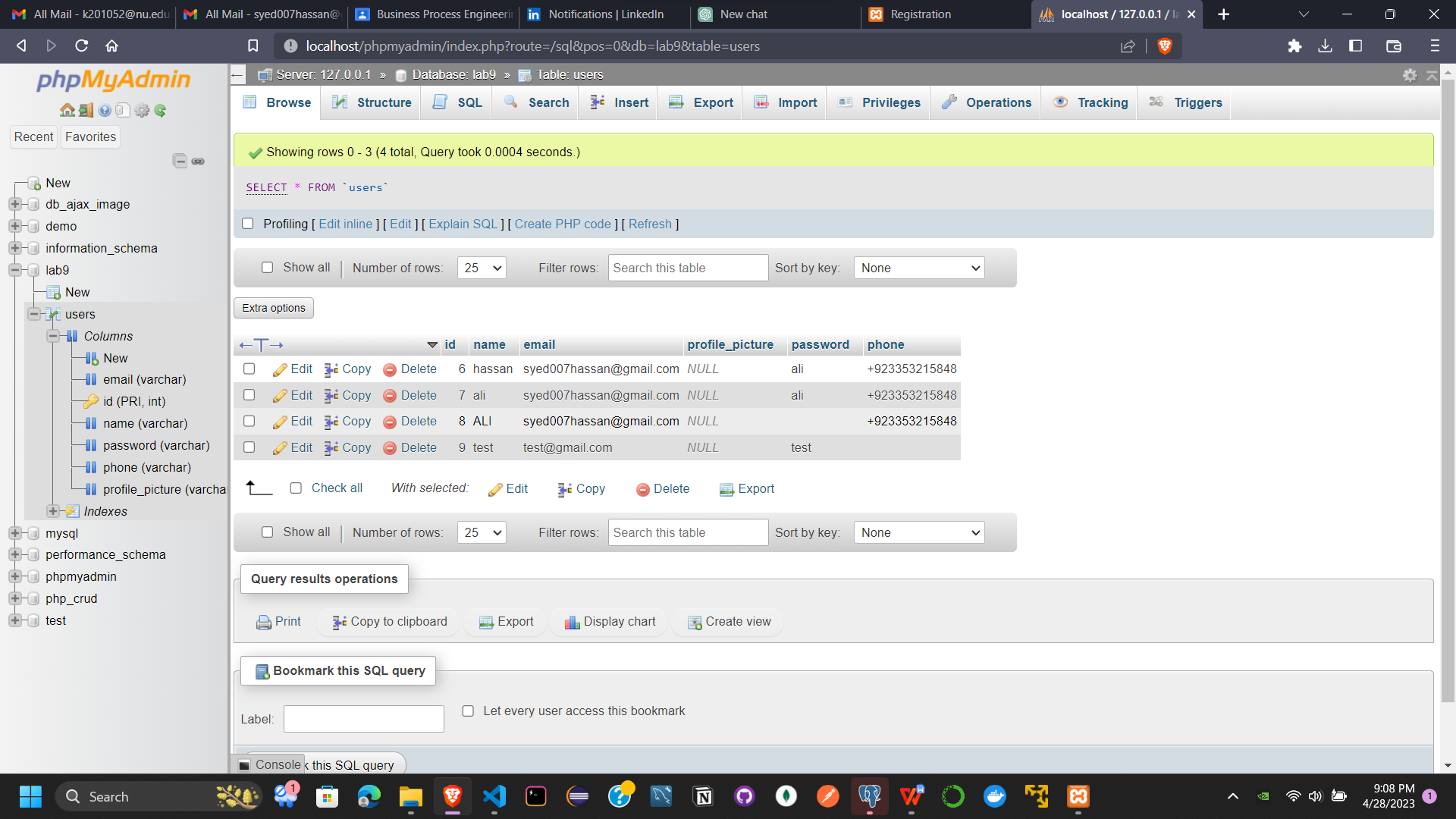
    </form>

</body>

</html>







Q4.

<?php

if (isset($\_COOKIE['last\_page'])) {

    echo "Welcome back! You have visited again ";

} else {

    echo "Welcome! This is your first visit.";

}

if (isset($\_SERVER['HTTP\_REFERER'])) {

    $last\_page = $\_SERVER['HTTP\_REFERER'];

} else {

    $last\_page = "";

}

setcookie("last\_page", $last\_page, time() + (86400 \* 30), "/"); // cookie lasts for 30 days

?>

<!DOCTYPE html>

<html>

<head>

    <title>Page 1</title>

</head>

<body>

    <h1>Welcome to Page 1</h1>

    <p>Click the button below to visit Page 2.</p>

    <a href="task4\_page2.php">Go to Page 2</a>

</body>

</html>

<?php

if (isset($\_COOKIE['last\_page'])) {

    echo "Welcome back! Your last visited page was: " . $\_COOKIE['last\_page'];

} else {

    echo "Welcome! This is your first visit.";

}

if (isset($\_SERVER['HTTP\_REFERER'])) {

    $last\_page = $\_SERVER['HTTP\_REFERER'];

} else {

    $last\_page = "";

}

setcookie("last\_page", $last\_page, time() + (86400 \* 30), "/"); // cookie lasts for 30 days

?>

<!DOCTYPE html>

<html>

<head>

    <title>Page 2</title>

</head>

<body>

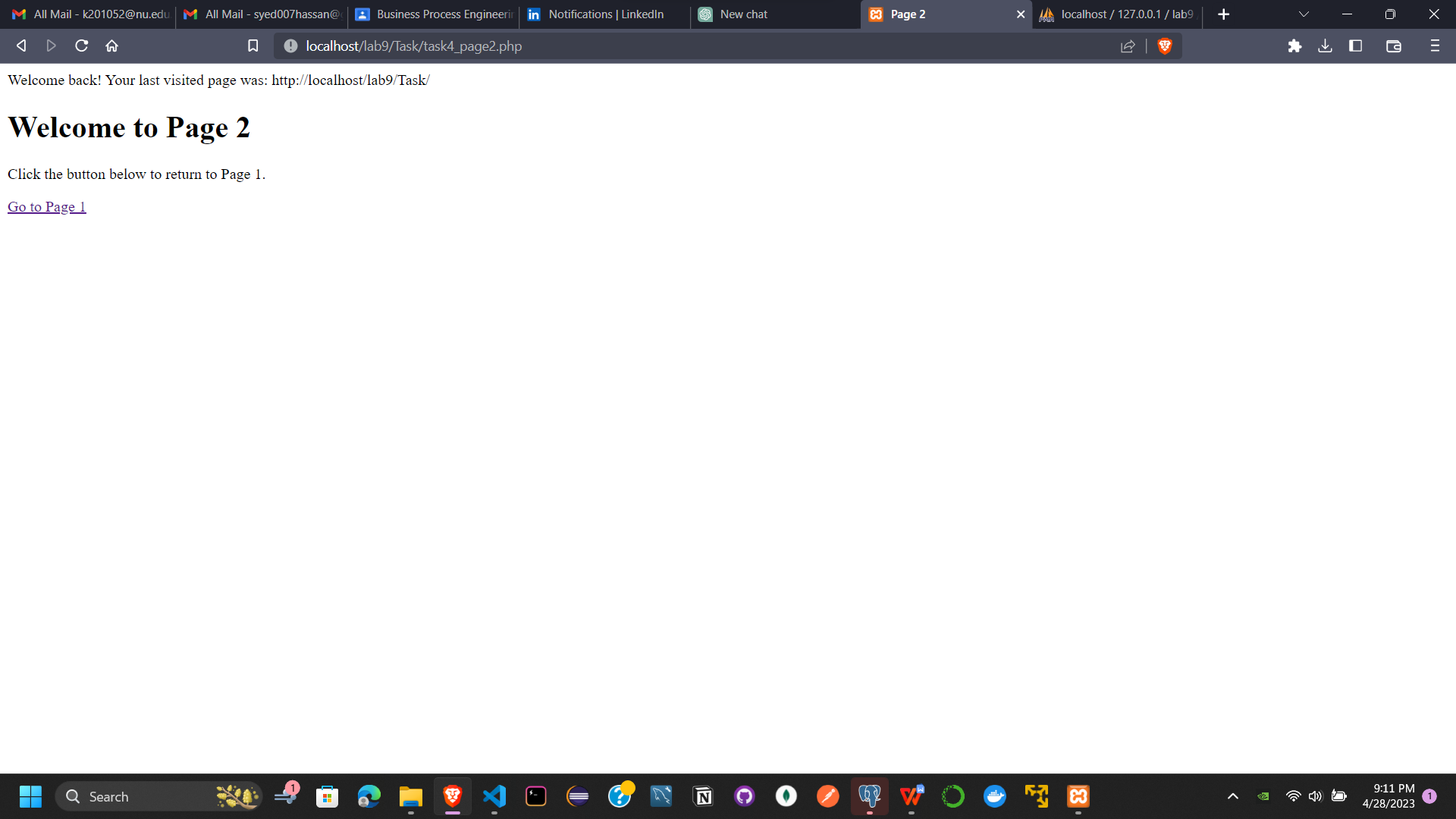
    <h1>Welcome to Page 2</h1>

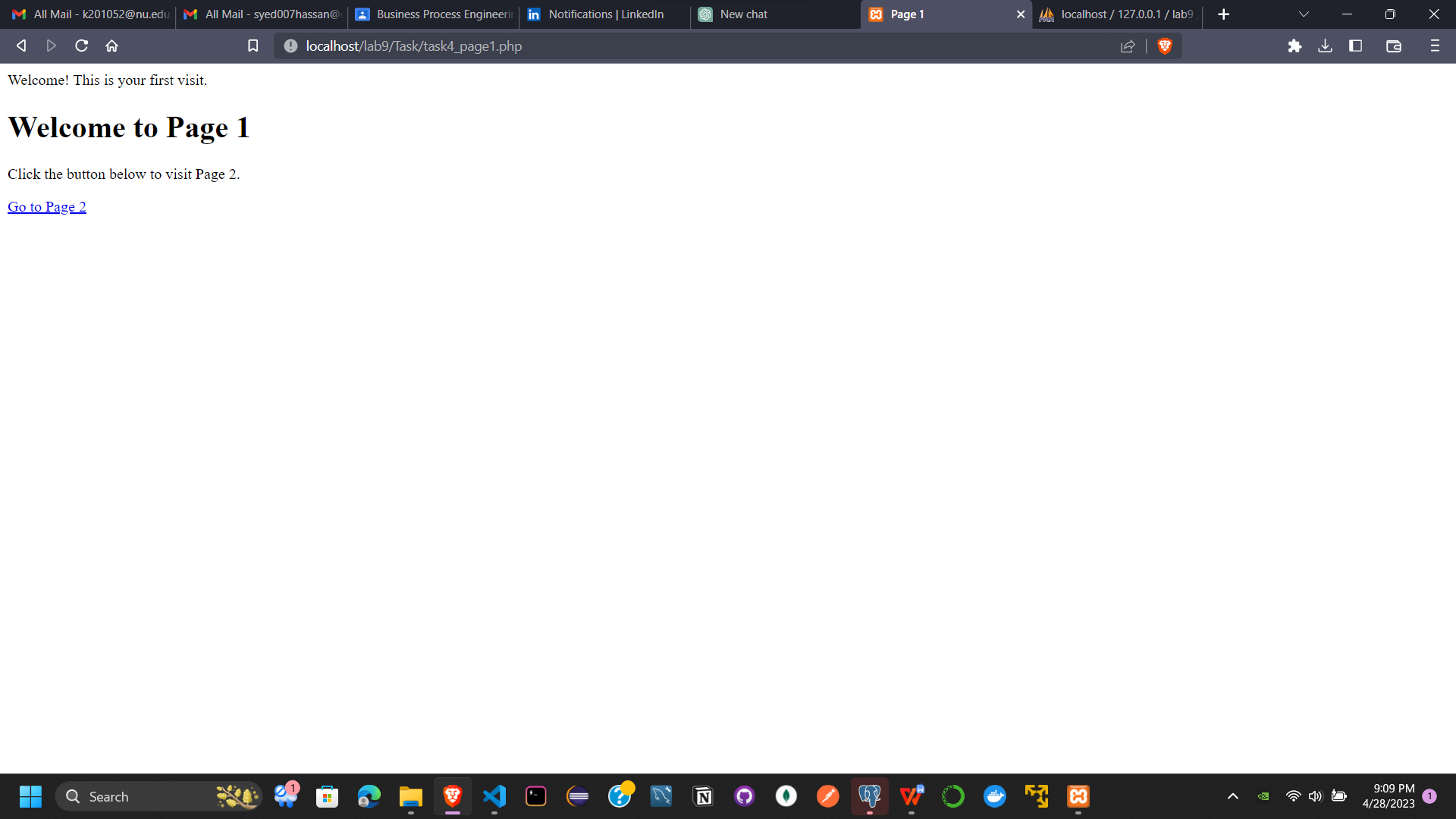
    <p>Click the button below to return to Page 1.</p>

    <a href="task4\_page1.php">Go to Page 1</a>

</body>

</html>





Q5.

<?php

session\_start();

require\_once('config.php');

$user\_id = 1;

$query = "SELECT \* FROM users WHERE id = ?";

$stmt = $conn->prepare($query);

$stmt->execute([$user\_id]);

$user = $stmt->fetch();

if (isset($\_POST['submit'])) {

    $name = $\_POST['name'];

    $email = $\_POST['email'];

    $query = "UPDATE users SET name = ?, email = ? WHERE id = ?";

    $stmt = $conn->prepare($query);

    $stmt->execute([$name, $email, $user\_id]);

    $file\_name = $\_FILES['profile\_picture']['name'];

    $file\_size = $\_FILES['profile\_picture']['size'];

    $file\_tmp = $\_FILES['profile\_picture']['tmp\_name'];

    $file\_type = $\_FILES['profile\_picture']['type'];

    $file\_ext = strtolower(end(explode('.', $file\_name)));

    $allowed\_exts = array('jpg', 'jpeg', 'png', 'gif');

    if (!in\_array($file\_ext, $allowed\_exts)) {

        $error\_msg = 'File must be an image (JPG, JPEG, PNG, or GIF).';

    } else {

        $upload\_dir = 'profile\_pictures/';

        $file\_new\_name = uniqid() . '.' . $file\_ext;

        $upload\_path = $upload\_dir . $file\_new\_name;

        move\_uploaded\_file($file\_tmp, $upload\_path);

        $query = "UPDATE users SET profile\_picture = ? WHERE id = ?";

        $stmt = $conn->prepare($query);

        $stmt->execute([$upload\_path, $user\_id]);

        header('Location: profile.php?success=1');

        exit();

    }

}

?>

<!DOCTYPE html>

<html>

<head>

    <title>My Profile</title>

</head>

<body>

    <h1>My Profile</h1>

    <?php if (isset($\_GET['success'])) : ?>

        <p class="success">Profile updated successfully.</p>

    <?php endif; ?>

    <form method="POST" enctype="multipart/form-data">

        <p>

            <label>Name:</label>

            <input type="text" name="name" value="<?php echo isset($user['name']) ? $user['name'] : ''; ?>">

        </p>

        <p>

            <label>Email:</label>

            <input type="email" name="email" value="<?php echo isset($user['email']) ? $user['email'] : ''; ?>">

        </p>

        <p>

            <label>Profile Picture:</label>

            <?php if (isset($user['profile\_picture']) && $user['profile\_picture']) : ?>

                <img src="<?php echo $user['profile\_picture']; ?>" alt="Profile Picture">

            <?php endif; ?>

        </p>

        <p>

            <label>Upload New Picture:</label>

            <input type="file" name="profile\_picture">

        </p>

        <?php if (isset($error\_msg)) : ?>

            <p class="error"><?php echo $error\_msg; ?></p>

        <?php endif; ?>

        <p>

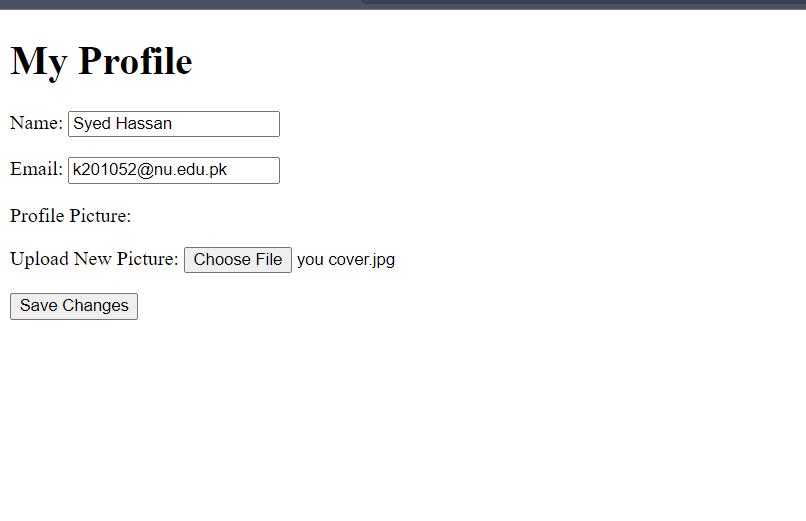
            <button type="submit" name="submit">Save Changes</button>

        </p>

    </form>

</body>

</html>



Q6.

<?php

include 'config.php';

$query = isset($\_GET['query']) ? $\_GET['query'] : '';

$search\_term = $query;

$results\_per\_page = 1;

$current\_page = isset($\_GET['page']) ? $\_GET['page'] : 1;

$starting\_limit = ($current\_page - 1) \* $results\_per\_page;

$stmt = $conn->prepare("SELECT \* FROM users WHERE name LIKE ? OR email LIKE ? LIMIT ?, ?");

$stmt->bind\_param('ssii', $search\_term, $search\_term, $starting\_limit, $results\_per\_page);

$stmt->execute();

$results = $stmt->get\_result()->fetch\_all(MYSQLI\_ASSOC);

$stmt = $conn->prepare("SELECT COUNT(\*) as count FROM users WHERE name LIKE ? OR email LIKE ?");

$stmt->bind\_param('ss', $search\_term, $search\_term);

$stmt->execute();

$total\_results = $stmt->get\_result()->fetch\_assoc()['count'];

$total\_pages = ceil($total\_results / $results\_per\_page);

if ($total\_results > 0) : ?>

    <table>

        <thead>

            <tr>

                <th>ID</th>

                <th>Name</th>

                <th>Email</th>

            </tr>

        </thead>

        <tbody>

            <?php foreach ($results as $result) : ?>

                <tr>

                    <td><?php echo $result['id']; ?></td>

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

                    <td><?php echo $result['email']; ?></td>

                </tr>

            <?php endforeach; ?>

        </tbody>

    </table>

    <br>

    <?php if ($total\_pages > 1) : ?>

        <div class="pagination">

            <?php if ($current\_page != 1) : ?>

                <a href="?search\_term=<?php echo $search\_term ?>&page=<?php echo $current\_page - 1 ?>">Previous</a>

            <?php endif; ?>

            <?php for ($i = 1; $i <= $total\_pages; $i++) : ?>

                <?php if ($i == $current\_page) : ?>

                    <span class="current-page"><?php echo $i ?></span>

                <?php else : ?>

                    <a href="?search\_term=<?php echo $search\_term ?>&page=<?php echo $i ?>"><?php echo $i ?></a>

                <?php endif; ?>

            <?php endfor; ?>

            <?php if ($current\_page != $total\_pages) : ?>

                <a href="?search\_term=<?php echo $search\_term ?>&page=<?php echo $current\_page + 1 ?>">Next</a>

            <?php endif; ?>

        </div>

    <?php endif; ?>

<?php else : ?>

    <p>No results found</p>

<?php endif; ?>

<style>

    table {

        border-collapse: collapse;

        width: 100%;

        margin: 20px 0;

        font-size: 1em;

        font-family: sans-serif;

    }

    table thead {

        background-color: #f2f2f2;

    }

    table th,

    table td {

        padding: 12px 15px;

        text-align: left;

        border-bottom: 1px solid #ddd;

    }

    table th {

        font-weight: bold;

        color: #555;

    }

    table tbody tr:hover {

        background-color: #f5f5f5;

    }

    .pagination {

        display: flex;

        justify-content: center;

        align-items: center;

        margin-top: 20px;

        font-size: 1.2em;

    }

    .pagination a,

    .current-page {

        color: #666;

        padding: 8px 16px;

        border: 1px solid #ddd;

        text-decoration: none;

    }

    .pagination a:hover {

        background-color: #ddd;

    }

    .current-page {

        background-color: #007bff;

        color: #fff;

        border: none;

    }

</style>

