

**WEB APP DEVELOPMENT**

**BSCS-4**

**Lab 12**

**Name:** Eshal Siraj

**Sap ID:** 54686

**Submitted to:** Mam Nayab Khalid

**ADD:**

<?php

include 'connect.php'; // Include database connection

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

    $name = mysqli\_real\_escape\_string($conn, $\_POST['sname']);

    $address = mysqli\_real\_escape\_string($conn, $\_POST['saddress']);

    $class = mysqli\_real\_escape\_string($conn, $\_POST['class']);

    $phone = mysqli\_real\_escape\_string($conn, $\_POST['sphone']);

    // Insert query

    $sql = "INSERT INTO users (sname, saddress, class, sphone) VALUES ('$name', '$address', '$class', '$phone')";

    if (mysqli\_query($conn, $sql)) {

        header("Location: index.php"); // Redirect to the home page

    } else {

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

    }

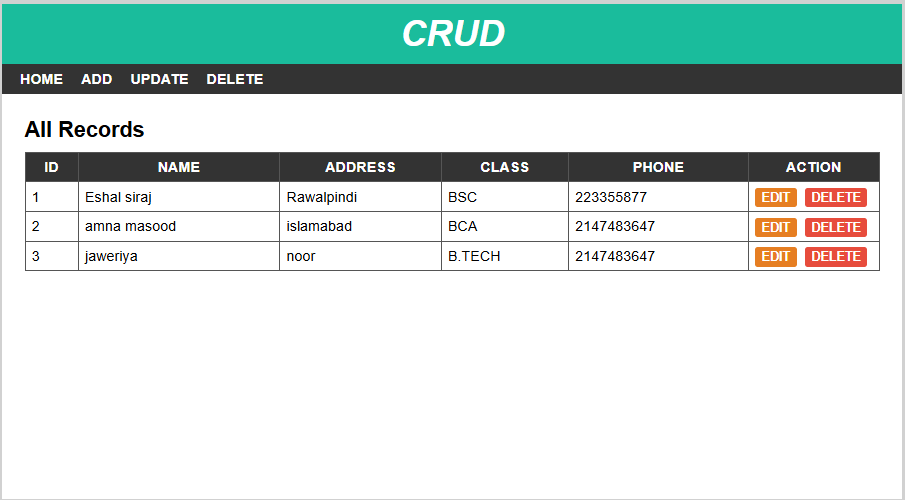
    mysqli\_close($conn);

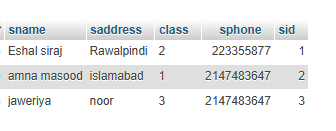
} else {

    echo "Invalid Request";

}

?>





**DELETE:**

<?php

include 'header.php';

include 'connect.php';

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

    $id = $\_POST['sid'];

    $sql = "DELETE FROM users WHERE sid = ?";

    $stmt = $conn->prepare($sql);

    $stmt->bind\_param("i", $id);

    if ($stmt->execute()) {

        echo "<p>Record deleted successfully.</p>";

    } else {

        echo "<p>Error deleting record: " . $conn->error . "</p>";

    }

    $stmt->close();

}

?>

<div id="main-content">

    <h2>Delete Record</h2>

    <form class="post-form" action="" method="post">

        <div class="form-group">

            <label>Id</label>

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

        </div>

        <input class="submit" type="submit" name="deletebtn" value="Delete" />

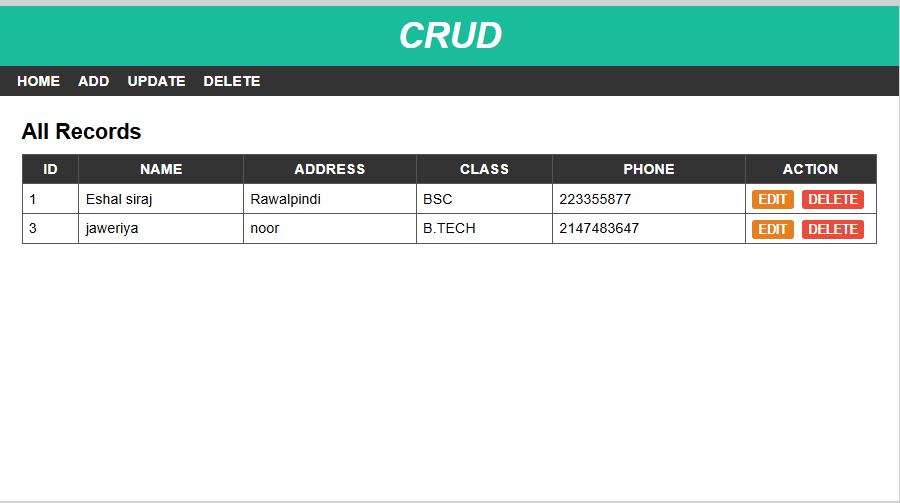
    </form>

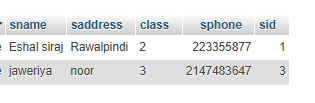
</div>

</div>

</body>

</html>





**UPDATE:**

<?php

include 'header.php';

include 'connect.php';

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

    $id = $\_GET['id'];

    $sql = "SELECT \* FROM users WHERE sid = ?";

    $stmt = $conn->prepare($sql);

    $stmt->bind\_param("i", $id);

    $stmt->execute();

    $result = $stmt->get\_result();

    if ($result->num\_rows > 0) {

        $row = $result->fetch\_assoc();

    } else {

        echo "<p>Record not found.</p>";

        exit;

    }

    $stmt->close();

}

?>

<div id="main-content">

    <h2>Update Record</h2>

    <form class="post-form" action="updatedata.php" method="post">

        <div class="form-group">

            <label>Name</label>

            <input type="hidden" name="sid" value="<?php echo $row['sid']; ?>" />

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

        </div>

        <div class="form-group">

            <label>Address</label>

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

        </div>

        <div class="form-group">

            <label>Class</label>

            <select name="sclass" required>

                <option value="1" <?php if ($row['class'] == 1) echo 'selected'; ?>>BCA</option>

                <option value="2" <?php if ($row['class'] == 2) echo 'selected'; ?>>BSC</option>

                <option value="3" <?php if ($row['class'] == 3) echo 'selected'; ?>>B.TECH</option>

            </select>

        </div>

        <div class="form-group">

            <label>Phone</label>

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

        </div>

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

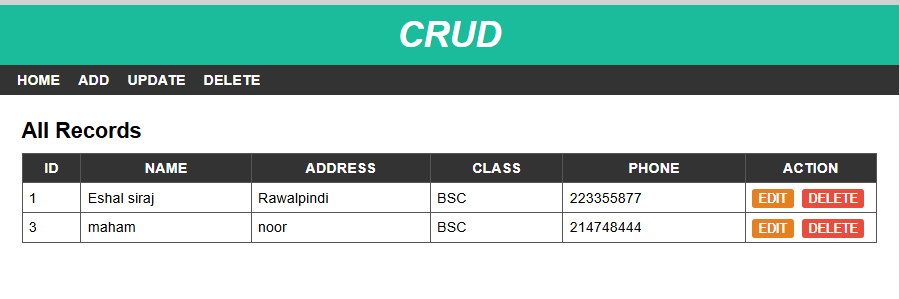
    </form>

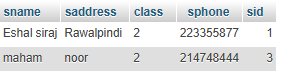
</div>

</div>

</body>

</html>

****

****

**READ:**

<?php

include 'header.php';

include 'connect.php'; // Include database connection

?>

<div id="main-content">

    <h2>All Records</h2>

    <table cellpadding="7px">

        <thead>

        <th>Id</th>

        <th>Name</th>

        <th>Address</th>

        <th>Class</th>

        <th>Phone</th>

        <th>Action</th>

        </thead>

        <tbody>

        <?php

        $sql = "SELECT \* FROM users";

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

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

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

                $className = '';

                if ($row['class'] == 1) {

                    $className = 'BCA';

                } elseif ($row['class'] == 2) {

                    $className = 'BSC';

                } elseif ($row['class'] == 3) {

                    $className = 'B.TECH';

                } else {

                    $className = 'Unknown';

                }

                echo "<tr>

                    <td>{$row['sid']}</td>

                    <td>{$row['sname']}</td>

                    <td>{$row['saddress']}</td>

                    <td>{$className}</td>

                    <td>{$row['sphone']}</td>

                    <td>

                        <a href='edit.php?id={$row['sid']}'>Edit</a>

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

                    </td>

                </tr>";

            }

        } else {

            echo "<tr><td colspan='6'>No Records Found</td></tr>";

        }

        ?>

        </tbody>

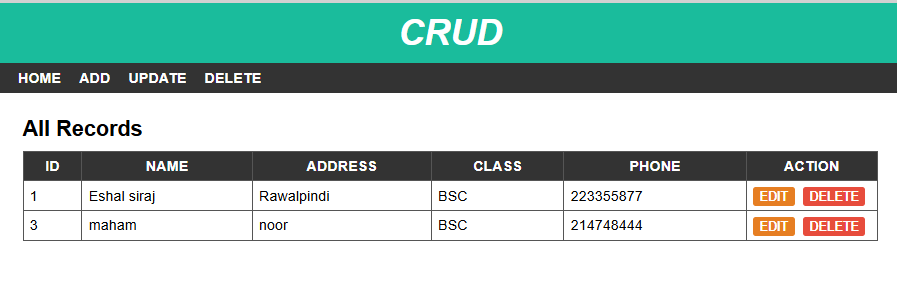
    </table>

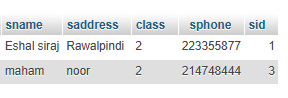
</div>

</div>

</body>

</html>

****

****