```
//add.php
<?php
//provide your hostname, username and dbname
include 'conn.php';
include("auth.php");
$user_name = $_POST['username'];
$sql = "select firstname, lastname, username from users where firstname LIKE '$user_name%'";
$result = mysqli_query($mysqli, $sql);
while($row = mysqli_fetch_array($result))
{
echo "<p>".$row['firstname']." ".$row['lastname']."</p>";
}
?>

//auth.php
<?php
session_start();
if(!isset($_SESSION["username"])){
header("Location: login.php");
exit(); }
?>

//conn.php

<?php
$host = "localhost";
$db_name = "mydb";
$username = "root";
$password = "";

//connect to mysql server
```

```
$mysqli = new mysqli($host, $username, $password, $db_name);

//check if any connection error was encountered
if(mysqli_connect_errno()) {
   echo "Error: Could not connect to database.";
   exit;
}
else
            echo "Connected to database.";
?>

//delete.php

<?php
include 'conn.php';
// delete sql query
$sql = "DELETE FROM users WHERE id = ?";

// prepare the sql statement
if($stmt = $mysqli->prepare($sql)){

   // bind the id of the record to be deleted
   // we use "i" here for integer
   $stmt->bind_param("i", $_GET['id']);

   // execute the delete statement
   if($stmt->execute()){

      // close the prepared statement
      $stmt->close();
            // redirect to index page
```

```
        // parameter "action=deleted" is used to show that something was deleted
        header('Location: index.php?action=deleted');


    }else{
        die("Unable to delete.");
    }
}
?>

//edit.php
<!DOCTYPE HTML>
<html>
    <head>
        <title>Update</title>
    </head>
<body>
<?php

include 'conn.php';
include 'auth.php';
?>
<h1>Update a Record</h1>
<div class="form">
<p>Welcome <?php echo $_SESSION['username']; ?>!</p>
<a href="logout.php">Logout</a>
</div>
<?php

// if the form was submitted/posted, update the record
if($_POST){
```

```
   //write query
   $sql = "UPDATE users SET firstname = ?, lastname = ?, username = ?, password  = ? WHERE id= ?";

   $stmt = $mysqli->prepare($sql);

   $stmt->bind_param('ssssi', $_POST['firstname'], $_POST['lastname'], $_POST['username'],
$_POST['password'], $_POST['id']);
      // execute the update statement
   if($stmt->execute()){
      echo "User was updated.";

      // close the prepared statement
      $stmt->close();
   }else{
      die("Unable to update.");
   }
}

$id=$_GET['id'];
/*
$sql = "SELECT id, firstname, lastname, username, password FROM users WHERE id =$id";

$result = $mysqli->query( $sql );
*/
$sql = "SELECT id, firstname, lastname, username, password FROM users WHERE id =?";
$stmt = $mysqli->prepare($sql);

   $stmt->bind_param('i', $id);
         $stmt->execute();
$result = $stmt->get_result();
```

```
$stmt->close();
$row = $result->fetch_assoc();

// php's extract() makes $row['firstname'] to $firstname automatically
extract($row);

//disconnect from database
$result->free();
$mysqli->close();

?>

<!--we have our html form here where new user information will be entered-->
<form action='edit.php?id=<?php echo $id; ?>' method='post' border='0'>
  <table>
    <tr>
      <td>Firstname</td>
      <td><input type='text' name='firstname' value='<?php echo $firstname;  ?>' /></td>
    </tr>
    <tr>
      <td>Lastname</td>
      <td><input type='text' name='lastname' value='<?php echo $lastname;  ?>' /></td>
    </tr>
    <tr>
      <td>Username</td>
      <td><input type='text' name='username'  value='<?php echo $username;  ?>' /></td>
    </tr>
    <tr>
      <td>Password</td>
      <td><input type='password' name='password'  value='<?php echo $password;  ?>' /></td>
    <tr>
```

```
        <td></td>
        <td>
            <input type='hidden' name='id' value='<?php echo $id ?>' />
            <input type='submit' value='Edit' />
            <a href='index.php'>Back to index</a>
        </td>
    </tr>
  </table>
</form>
</body>
</html>

//index.php
<!DOCTYPE HTML>
<html>
  <head>
    <title>Read Records</title>
  </head>
<body>
<?php
include("auth.php");
?>
<h1>Read Records</h1>
<div>
<p>Welcome <?php echo $_SESSION['username']; ?>!</p>
<p>This is secure area.</p>

<a href="logout.php">Logout</a>
</div>
<?php
```

```
include 'conn.php';
if(isset($_GET['action']))
$action=$_GET['action'];
else $action="";
//if the user clicked ok, run our delete query
if($action=='deleted'){
   echo "User was deleted.";
}

$query = "select * from users";
$stmt = $mysqli->prepare($query);



            $stmt->execute();
$result = $stmt->get_result();
$stmt->close();
//$result = $mysqli->query( $query );

$num_results = $result->num_rows;

echo "<div><a href='add.php'>Create New Record</a></div>";

if( $num_results ){
   echo "<table border='1'>";

      echo "<tr>";
         echo "<th>Firstname</th>";
         echo "<th>Lastname</th>";
         echo "<th>Username</th>";
                              echo "<th>Profile Picture</th>";
         echo "<th>Action</th>";
```

```
        echo "</tr>";



    while( $row = $result->fetch_assoc() ){

        //extract row
        //this will make $row['firstname'] to just $firstname only
        extract($row);

        //creating new table row per record
        echo "<tr>";
            echo "<td>{$firstname}</td>";
            echo "<td>{$lastname}</td>";
            echo "<td>{$username}</td>";
                                    echo "<td>
                                    <img height='100px' width='100px' src=\"{$profilepic}\"/>
                                    </td>";
                                    ?>
                                    <?php
            echo "<td>";
                echo "<a href='edit.php?id={$id}'>Edit</a>";
                //echo " / ";

                // delete_user is a javascript function, see at the bottom par of the page
                echo "<a href='#' onclick='delete_user( {$id} );'>Delete</a>";
            echo "</td>";
        echo "</tr>";
    }
    //end table
    echo "</table>";
}
```

```
//if table is empty
else{
   echo "No records found.";
}
$result->free();
$mysqli->close();
?>

<script type='text/javascript'>
function delete_user( id ){

   var answer = confirm('Are you sure?');

   //if user clicked ok
   if ( answer ){
      //redirect to url with action as delete and id to the record to be deleted
      window.location = 'delete.php?id=' + id;
   }
}
function user_suggestion()
{
var user = document.getElementById("user").value;
var xhr;
 if (window.XMLHttpRequest) { // Mozilla, Safari, ...
   xhr = new XMLHttpRequest();
} else if (window.ActiveXObject) { // IE 8 and older
   xhr = new ActiveXObject("Microsoft.XMLHTTP");
}
var data = "username=" + user;
    xhr.open("POST", "search.php", true);
    xhr.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
```

```
    xhr.send(data);
            xhr.onreadystatechange = display_data;
           function display_data() {
            if (xhr.readyState == 4) {
     if (xhr.status == 200) {
      //alert(xhr.responseText);
             document.getElementById("suggestion").innerHTML = xhr.responseText;
     } else {
       alert('There was a problem with the request.');
     }
    }
          }
}
</script>

<h1>Search User Record</h1>
<div>
<form>
          <br/><br/>
                    <label for="book">Search User </label>
                    <div>
                    <input type="text" id="user" onKeyUp="user_suggestion()">
                    <div id="suggestion"></div>
                    </div>
                    <!--<input name="submit" type="submit" value="Submit" />-->
          </form>
</div>
</body>
</html>

//login.php
```

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>Login</title>
<link rel="stylesheet" href="main.css" />
</head>
<body>
<?php
require('conn.php');
session_start();
// If form submitted, insert values into the database.
if (isset($_POST['username'])){
      // removes backslashes
          $username = stripslashes($_REQUEST['username']);
      //escapes special characters in a string
                  //https://www.php.net/manual/en/mysqli.real-escape-string.php
          $username = mysqli_real_escape_string($mysqli,$username);
          $password = stripslashes($_REQUEST['password']);
          $password = mysqli_real_escape_string($mysqli,$password);
          //Checking is user existing in the database or not
      $query = "SELECT * FROM `users` WHERE username='$username'
and password='$password'";
          $result = mysqli_query($mysqli,$query) or die(mysql_error());
          $rows = mysqli_num_rows($result);
      if($rows==1){if(!isset($_SESSION['username'])){
              $_SESSION['username'] = $username;}
         // Redirect user to index.php
              header("Location: index.php");
                  //echo $_SESSION['username'];
       }else{
```

```
            echo "<div class='form'>
<h3>Username/password is incorrect.</h3>
<br/>Click here to <a href='login.php'>Login</a></div>";
            }
    }else{
?>
<div class="form">
<h1>Log In</h1>
<form action="" method="post" name="login">
<input type="text" name="username" placeholder="Username" required />
<input type="password" name="password" placeholder="Password" required />
<input name="submit" type="submit" value="Login" />
</form>
<p>Not registered yet? <a href='add.php'>Register Here</a></p>
</div>
<?php } ?>
</body>
</html>

//logout.php

<?php
session_start();
session_destroy();
header("Location: login.php");

?>

//search.php

<?php
```

```
//provide your hostname, username and dbname
include 'conn.php';
include("auth.php");
$user_name = $_POST['username'];
$sql = "select firstname, lastname, username from users where firstname LIKE '$user_name%'";
$result = mysqli_query($mysqli, $sql);
while($row = mysqli_fetch_array($result))
{
echo "<p>".$row['firstname']." ".$row['lastname']."</p>";
}
?>
```