Upload

<?php require\_once('../Connections/Jayant.php'); ?>

<?php

//initialize the session

if (!isset($\_SESSION)) {

session\_start();

}

// \*\* Logout the current user. \*\*

$logoutAction = $\_SERVER['PHP\_SELF']."?doLogout=true";

if ((isset($\_SERVER['QUERY\_STRING'])) && ($\_SERVER['QUERY\_STRING'] != "")){

$logoutAction .="&". htmlentities($\_SERVER['QUERY\_STRING']);

}

if ((isset($\_GET['doLogout'])) &&($\_GET['doLogout']=="true")){

//to fully log out a visitor we need to clear the session varialbles

$\_SESSION['MM\_Username'] = NULL;

$\_SESSION['MM\_UserGroup'] = NULL;

$\_SESSION['PrevUrl'] = NULL;

unset($\_SESSION['MM\_Username']);

unset($\_SESSION['MM\_UserGroup']);

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

$logoutGoTo = "welcome.php";

if ($logoutGoTo) {

header("Location: $logoutGoTo");

exit;

}

}

?>

<?php

if (!isset($\_SESSION)) {

session\_start();

}

$MM\_authorizedUsers = "";

$MM\_donotCheckaccess = "true";

// \*\*\* Restrict Access To Page: Grant or deny access to this page

function isAuthorized($strUsers, $strGroups, $UserName, $UserGroup) {

// For security, start by assuming the visitor is NOT authorized.

$isValid = False;

// When a visitor has logged into this site, the Session variable MM\_Username set equal to their username.

// Therefore, we know that a user is NOT logged in if that Session variable is blank.

if (!empty($UserName)) {

// Besides being logged in, you may restrict access to only certain users based on an ID established when they login.

// Parse the strings into arrays.

$arrUsers = Explode(",", $strUsers);

$arrGroups = Explode(",", $strGroups);

if (in\_array($UserName, $arrUsers)) {

$isValid = true;

}

// Or, you may restrict access to only certain users based on their username.

if (in\_array($UserGroup, $arrGroups)) {

$isValid = true;

}

if (($strUsers == "") && true) {

$isValid = true;

}

}

return $isValid;

}

$MM\_restrictGoTo = "welcome.php";

if (!((isset($\_SESSION['MM\_Username'])) && (isAuthorized("",$MM\_authorizedUsers, $\_SESSION['MM\_Username'], $\_SESSION['MM\_UserGroup'])))) {

$MM\_qsChar = "?";

$MM\_referrer = $\_SERVER['PHP\_SELF'];

if (strpos($MM\_restrictGoTo, "?")) $MM\_qsChar = "&";

if (isset($\_SERVER['QUERY\_STRING']) && strlen($\_SERVER['QUERY\_STRING']) > 0)

$MM\_referrer .= "?" . $\_SERVER['QUERY\_STRING'];

$MM\_restrictGoTo = $MM\_restrictGoTo. $MM\_qsChar . "accesscheck=" . urlencode($MM\_referrer);

header("Location: ". $MM\_restrictGoTo);

exit;

}

?>

<?php

if (!function\_exists("GetSQLValueString")) {

function GetSQLValueString($theValue, $theType, $theDefinedValue = "", $theNotDefinedValue = "")

{

if (PHP\_VERSION < 6) {

$theValue = get\_magic\_quotes\_gpc() ? stripslashes($theValue) : $theValue;

}

$theValue = function\_exists("mysql\_real\_escape\_string") ? mysql\_real\_escape\_string($theValue) : mysql\_escape\_string($theValue);

switch ($theType) {

case "text":

$theValue = ($theValue != "") ? "'" . $theValue . "'" : "NULL";

break;

case "long":

case "int":

$theValue = ($theValue != "") ? intval($theValue) : "NULL";

break;

case "double":

$theValue = ($theValue != "") ? doubleval($theValue) : "NULL";

break;

case "date":

$theValue = ($theValue != "") ? "'" . $theValue . "'" : "NULL";

break;

case "defined":

$theValue = ($theValue != "") ? $theDefinedValue : $theNotDefinedValue;

break;

}

return $theValue;

}

}

$editFormAction = $\_SERVER['PHP\_SELF'];

if (isset($\_SERVER['QUERY\_STRING'])) {

$editFormAction .= "?" . htmlentities($\_SERVER['QUERY\_STRING']);

}

if ((isset($\_POST["MM\_update"])) && ($\_POST["MM\_update"] == "form1")) {

$updateSQL = sprintf("UPDATE registration SET Reg=%s, name=%s, pass=%s, email=%s, Mobile\_no=%s WHERE ID\_no=%s",

GetSQLValueString($\_POST['Reg'], "int"),

GetSQLValueString($\_POST['name'], "text"),

GetSQLValueString($\_POST['pass'], "text"),

GetSQLValueString($\_POST['email'], "text"),

GetSQLValueString($\_POST['Mobile\_no'], "bigint"),

GetSQLValueString($\_POST['Pid'], "int"));

mysql\_select\_db($database\_Jayant, $Jayant);

$Result1 = mysql\_query($updateSQL, $Jayant) or die(mysql\_error());

$updateGoTo = "ud.php";

if (isset($\_SERVER['QUERY\_STRING'])) {

$updateGoTo .= (strpos($updateGoTo, '?')) ? "&" : "?";

$updateGoTo .= $\_SERVER['QUERY\_STRING'];

}

header(sprintf("Location: %s", $updateGoTo));

}

if ((isset($\_GET['ID\_no'])) && ($\_GET['ID\_no'] == "theValue")) {

$deleteSQL = sprintf("DELETE FROM registration WHERE ID\_no=%s",

GetSQLValueString($\_GET['ID\_no'], "int"));

mysql\_select\_db($database\_Jayant, $Jayant);

$Result1 = mysql\_query($deleteSQL, $Jayant) or die(mysql\_error());

$deleteGoTo = "ud.php";

if (isset($\_SERVER['QUERY\_STRING'])) {

$deleteGoTo .= (strpos($deleteGoTo, '?')) ? "&" : "?";

$deleteGoTo .= $\_SERVER['QUERY\_STRING'];

}

header(sprintf("Location: %s", $deleteGoTo));

}

if (isset ($\_POST["search"]))

{

$theValue = mysql\_real\_escape\_string($\_POST["theValue"]);

$query\_Recordset1 = "SELECT \* FROM registration WHERE ID\_no = '$theValue' OR Reg = '$theValue'";

}else{

echo 'Please enter valid pid';}

mysql\_select\_db($database\_Jayant, $Jayant);

$query\_Recordset1 = "SELECT \* FROM registration WHERE ID\_no = '$theValue' OR Reg = '$theValue'";

$Recordset1 = mysql\_query($query\_Recordset1, $Jayant) or die(mysql\_error());

$row\_Recordset1 = mysql\_fetch\_assoc($Recordset1);

$totalRows\_Recordset1 = mysql\_num\_rows($Recordset1);

?>

<!doctype html>

<html>

<head>

<meta charset="utf-8">

<link href="favicon.png" rel="icon" type="image/png" />

<title>Admin page</title>

<style type="text/css">

<!--

</style>

<link href="../CSS/j1.css" rel="stylesheet" type="text/css">

</head>

<body>

<div class="container">

<div class="header"><a href="#"><img src="../image/0.jpg" alt="Insert Logo Here" name="Insert\_logo" width="180" height="90" id="Insert\_logo" style="background-color:#00F; display:block;" /></a>

<!-- end .header --></div>

<div class="sidebar1">

<ul class="nav">

<li><a href="login1.php">Registration</a></li>

<li><a href="se.php">Search Detail</a></li>

<li><a href="ud.php">Update</a></li>

<li><a href="de.php">Delete</a></li>

<li><a href="#">Tweet Search </a></li>

<li><a href="<?php echo $logoutAction ?>">Log out</a></li>

</ul>

<!-- end .sidebar1 --></div>

<div class="content">

<div id="Sign-Up" align="center"><a href="<?php echo $logoutAction ?>">Log out</a>

<div align="left">

<div align="left">

<form name="theValue" method="POST" action="ud.php" min='1000' max='2000' required><table align="center"><tr><td><table align="left" background="../images/8.jpg" bordercolorlight="#FF0000" border="5"><tr><td colspan="5"><h5>Enter P.id OR Registration No</h5></td></tr>

<tr><td colspan="5"><input id="Text2" type="text" name="theValue" placeholder="Enter P.ID/Reg No."value='' min='1000' max='2000' required></td></tr><tr><td>

<button class=" button"type=" Submit" name="search" value="Search..."><span>Search Detail</span></button></td><td> <a href="Userreg.PHP">Back</a></td></tr></table>

</form> </fieldset></td>

</div>

</form>

<div align="right">

<fieldset style="width:60%" >

<legend><h5>Search Details</h5></legend>

<table border="0">

<tr>

<form method="post" name="form1" action="<?php echo $editFormAction; ?>">

<table align="center">

<tr valign="baseline">

<td nowrap align="right">Pid:</td>

<td><?php echo $row\_Recordset1['ID\_no']; ?></td>

</tr>

<tr valign="baseline">

<td nowrap align="right">Reg:</td>

<td><input type="text" name="Reg" value="<?php echo htmlentities($row\_Recordset1['Reg'], ENT\_COMPAT, 'utf-8'); ?>" size="32"></td>

</tr>

<tr valign="baseline">

<td nowrap align="right">Name:</td>

<td><input type="text" name="name" value="<?php echo htmlentities($row\_Recordset1['name'], ENT\_COMPAT, 'utf-8'); ?>" size="32"></td>

</tr>

<tr valign="baseline">

<td nowrap align="right">Email:</td>

<td><input type="text" name="email" value="<?php echo htmlentities($row\_Recordset1['email'], ENT\_COMPAT, 'utf-8'); ?>" size="32"></td>

</tr>

<tr valign="baseline">

<td nowrap align="right">Mobile\_no:</td>

<td><input type="text" name="Mobile\_no" value="<?php echo htmlentities($row\_Recordset1['Mobile\_no'], ENT\_COMPAT, 'utf-8'); ?>" size="32"></td>

</tr>

<tr valign="baseline">

<td nowrap align="right">&nbsp;</td>

<td><input type="submit" value="Update record"></td>

</tr>

</table>

<input type="hidden" name="MM\_update" value="form1">

<input type="hidden" name="Pid" value="<?php echo $row\_Recordset1['ID\_no']; ?>">

</form>

<p>&nbsp;</p>

</div>

</table>

<input type="hidden" name="MM\_insert" value="form">

</form>

</table>

</fieldset>

</div>

<!-- end .content --></div>

<div class="footer">

<p align="center">This Project for the testing purposes</p>

<!-- end .footer --></div>

<!-- end .container --></div>

<?php echo $row\_Recordset1['ID\_no']; ?>

</body>

</html>

<?php

mysql\_free\_result($Recordset1);

?>