Add

$firstname = $\_POST['firstname'];

$lastname = $\_POST['lastname'];

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

$password = $\_POST['password'];

$usertype = "USER";

$dir = "images/";

$target\_file = $dir.basename($\_FILES["image"]["name"]);

$imageFileType = pathinfo($target\_file,PATHINFO\_EXTENSION);

$file=$\_FILES['image']['tmp\_name'];

$picture=$\_FILES['image']['name'];

if($picture == "")

{

echo "<script>alert('Please choose a picture!')</script>";

} else {

if($imageFileType != "jpg" && $imageFileType != "png" && $imageFileType != "jpeg") {

echo "<script>alert('PNG, JPG, and JPEG are allowed!')</script>";

} else {

$image= addslashes(file\_get\_contents($\_FILES['image']['tmp\_name']));

$image\_name= addslashes($\_FILES['image']['name']);

move\_uploaded\_file($\_FILES["image"]["tmp\_name"], $dir . $\_FILES["image"]["name"]);

$query = "INSERT INTO accounts(id,firstname,lastname,username,password,picture,usertype) VALUES (null,'".$firstname."','".$lastname."','".$username."','".$password."','".$picture."','".$usertype."')";

mysqli\_query($db,$query);

echo "<script>alert('Data Successfully Saved!')</script>";

echo '<script>windows: location="view\_accounts.php"</script>';

}

}

}

?>

<form method="post" action="Canteen.php" onsubmit="return(valid());">

<table border="1" align="center" width="500" cellpadding="10" cellspacing="10">

<tr>

<td>

<table align="center" cellpadding="10" cellspacing="10" width="400">

<?php

if(isset($\_REQUEST['message']))

{

$msg=$\_REQUEST['message'];

echo'<tr><td colspan="2" style="color:#FF0000" align="center">'.$msg.'</td></tr>';

}

?>

<tr>

<td colspan="2" align="center">&nbsp;</td>

</tr>

<tr>

<h3 class="tittle two"><u>LOGIN</u></h3>

</tr>

<tr>

<td>User Name</td>

<td><input type="text" name="name" class="form-control" id="u" placeholder="user name"></td>

</tr>

<tr>

<td>Password</td>

<td><input type="password" name="Mobile\_no" class="form-control" id="p" placeholder="Password"></td>

</tr>

<tr>

<td colspan="2" align="center"><input type="submit" name="submit" value="Login"/> </td>

</tr>

<tr>

<td colspan="2" align="center">&nbsp;</td>

</tr>

</table>

</td>

</tr>

</table>

<?php

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

{

$myuser=$\_POST['name'];

$mypass=$\_POST['password'];

$\_SESSION['name']=$\_POST['name'];

$\_SESSION['pass']=$\_POST['password'];

$sql="SELECT \* FROM `admin` where name='$myuser' and password='$mypass'";

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

$row=mysqli\_fetch\_array($result,MYSQLI\_ASSOC);

$count=mysqli\_num\_rows($result);

if ($count==1)

{

$\_SESSION['id']=$row['id'];

header("students record.php");

}

else

{

?>

<script>

alert("invalid username or password");

</script>

<?php

}

}

?>