<?php

require '../bootstrap.php';

session\_start();

if(empty($\_SESSION['id\_pengguna']))

{

header('location:~/../../index.php');

}

?>

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

<?php

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

{

$oldpass = $\_POST["oldpass"];

$newpass = $\_POST["newpass"];

$confirmpass = $\_POST["confirmpass"];

$user\_id = $\_SESSION['id\_pengguna'];

include 'dbconnect.php';

$sql2 = "SELECT id\_penyewa,no\_ic,kata\_laluan FROM penyewa

WHERE no\_ic = '$user\_id'";

$result = mysql\_query($sql2) or die('Query failed. ' . mysql\_error());

$row = mysql\_fetch\_array($result, MYSQL\_ASSOC);

$password = $row['kata\_laluan'];

if ($oldpass == "" && $newpass == "" && $confirmpass == "")

{

echo "<script languange = 'Javascript'>

alert('Sila isi semua ruang dibawah');

location.href = 'tukar\_kata\_laluan.php';

</script>";

}

elseif ($oldpass != $password)

{

echo "<script languange = 'Javascript'>

alert('Kata Laluan Asal tidak tepat');

location.href = 'tukar\_kata\_laluan.php';

</script>";

}

elseif ($newpass != $confirmpass)

{

echo "<script languange = 'Javascript'>

alert('Sah Kata Laluan salah');

location.href = 'tukar\_kata\_laluan.php';

</script>";

}

else

{

$sql = "UPDATE penyewa SET kata\_laluan = '$newpass' WHERE no\_ic = '$user\_id'";

mysql\_query($sql) or die(mysql\_error());

echo "<script languange = 'Javascript'>

alert('Kata Laluan berjaya ditukar');

location.href = 'tukar\_kata\_laluan.php';

</script>";

}

}

?>

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

<?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;

}

}

$colname\_Recordset1 = "-1";

if (isset($\_SESSION['id\_pengguna'])) {

$colname\_Recordset1 = $\_SESSION['id\_pengguna'];

}

mysql\_select\_db($database\_erental, $erental);

$query\_Recordset1 = sprintf("SELECT \* FROM penyewa WHERE no\_ic = %s", GetSQLValueString($colname\_Recordset1, "text"));

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

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

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

?>

<?php head(); ?>

<ul class="breadcrumb"><li><a href="#">Tukar Kata Laluan</a></li></ul>

<div class="accordion-group breadcrumb">

<legend style="color:#0066CC"><h3>Tukar Kata Laluan</h3></legend>

<form id="form1" name="form1" method="POST">

<table class="table table-bordered" width="386" border="0" align="center">

<tr>

<td height="35" colspan="2" align="center"><strong>Tukar Kata Laluan</strong></td>

</tr>

<tr>

<td> Kata laluan Asal</td>

<td><input type="password" name="oldpass" id="oldpass" /></td>

</tr>

<tr>

<td> Kata Laluan Baru</td>

<td><input type="password" name="newpass" id="newpass" /></td>

</tr>

<tr>

<td>Sah Kata laluan</td>

<td><input type="password" name="confirmpass" id="confirmpass" /></td>

</tr>

<tr>

<td>&nbsp;</td>

<td><input name="id\_penyewa" type="hidden" id="id\_penyewa" value="<?php echo $row\_Recordset1['id\_penyewa']; ?>" /></td>

</tr>

<tr>

<td>&nbsp;</td>

<td><input name="Submit" type="submit" class="btn btn-primary" id="Submit" value="Tukar" />

<input class="btn btn-primary" type="reset" name="Semula" id="Semula" value="Semula" /></td>

</tr>

</table>

<label for="oldpass"></label>

</form>

</div>

<?php footer()?>

<?php

mysql\_free\_result($Recordset1);

?>