```
<?php # chapter 10_ Review and Pursue - edit_customer.php
/*this page is for editing customer details including the password
*page accessed through view_customers.php
*Additionally _ if no details are changed a message is displayed
*This script was written in answer to the final pursue questions for Chpt 10
* Caveat: This does not represent any kind of real life scenario and is purely to demonstrate ideas
*/

//change page title to suit user to be edited as per Review and Pursue chapter 10
if ($_SERVER['REQUEST_METHOD']=='GET'){
@$page_title= 'Edit Customer: '. $_GET['fn'] . '  ' . $_GET['ln'];//suppress error messages if url retyped with gaps
}else{
$page_title='Edit Customer: ' . $_POST['first_name'] . ' ' . $_POST['last_name'];
}
include ('includes/header.html');
echo '<h1> Edit Customer Details</h1>';
require_once ('includes/mysqli_bank_connect.php');//connect to the db

//check for a valid user ID, first name, last name through GET or POST
if ((isset($_GET['id'])) && (is_numeric($_GET['id'])) && (isset($_GET['fn'])) && (isset($_GET['ln']))){//from view_users.php
	$id=$_GET['id'];
	$fn=$_GET['fn'];
	$ln=$_GET['ln'];
	$query="SELECT customer_id FROM customers WHERE customer_id='$id' AND first_name='$fn' AND last_name='$ln'";
	$result=mysqli_query($dbc, $query);
	if(mysqli_num_rows($result)!=1){
		echo '<p class="error">There has been an error accessing this page. Please return to the view customers page.</p>';
		mysqli_close($dbc);//kill the db connection
		include ('includes/footer.html');//footer
		exit();//kill the script

	}else{
		$id=$_GET['id'];
		$fn=$_GET['fn'];
		$ln=$_GET['ln'];
	}

}elseif((isset($_POST['id'])) && (is_numeric($_POST['id']))){//form submitted
	$id=$_POST['id'];
}else{//no valid ID: stop the script
	echo '<p class="error">This page has been accessed in error.</p>';
	include ('includes/footer.html');
	exit();

}//end check for submission type

//check if the form has been submitted rather than accessed from the view_customers.php page
if ($_SERVER['REQUEST_METHOD']=='POST'){

	$errors = array();

	//check for first name
	if (empty($_POST['first_name'])){
		$errors[] = 'You did not enter a first name.';
```

```
	}else{
		$fn = mysqli_real_escape_string($dbc, trim($_POST['first_name']));
	}//first name

	//check for a last name
	if (empty($_POST['last_name'])){
		$errors[] = 'You did not enter a last name';
	}else{
		$ln = mysqli_real_escape_string($dbc, trim($_POST['last_name']));
	}//last name

	//check current pin is given
	if (empty($_POST['pin'])){
		$errors[] = 'You did not enter your current pin';
	}else{//check to see if pin given matches the current pin for this customer_id
		$pin = mysqli_real_escape_string($dbc, trim($_POST['pin']));//entered pin
		$query="SELECT customer_id FROM customers WHERE customer_id='$id' AND
AES_DECRYPT(pin,nac1)=$pin";
		$result=mysqli_query($dbc, $query);
		if(mysqli_num_rows($result)!= 1){
			$errors[] = 'This pin does not match the current pin.
			Please go back and try again';
		}
	}

	//check for a new pin and match against the confirmed pin
	if(!empty($_POST['pin1'])){
		if ($_POST['pin1'] != $_POST['pin2']){
			$errors[] = 'Your new pin does not match the confirmed pin.';
		}else{
			$newpin = mysqli_real_escape_string($dbc, trim($_POST['pin1']));
			//test for unique customer first_name, last_name, pin combination as
entered
			$query = "SELECT customer_id FROM customers WHERE first_name='$fn'
AND last_name='$ln' AND AES_DECRYPT(pin,nac1)=$newpin";
			$result = @mysqli_query($dbc, $query);
			if(mysqli_num_rows($result)== 0){
				$pinOK = TRUE;
				}else{
					$errors[] = "This pin and name cannot be accepted. Please
try again";//this combination already exists
				}
		}
	}else{
		$errors[] = 'You did not enter your new pin.';//forgot to enter your pin, dunderheid!
	}

	if (empty($errors)){//no inputs missed

		if ($pinOK){//if the pin/name combo is OK
			//make the query
			$query = "UPDATE customers SET first_name='$fn', last_name='$ln', pin =
AES_ENCRYPT('$newpin', nac1)
					WHERE customer_id='$id' LIMIT 1";
			$result = @mysqli_query($dbc, $query);
			if (@mysqli_affected_rows($dbc)==1){//only one row changed is OK
				//display message
				echo '<p>The user record has been altered.</p>';
				mysqli_close($dbc);//kill the db connection
				include ('includes/footer.html');//footer
```

```
                        exit();//kill the script
                    }elseif(@mysqli_affected_rows($dbc)==0){//no row changed: no new
details
                        //display message
                        echo '<p>No new details have been inserted.</p>';
                        mysqli_close($dbc);//kill the db connection
                        include ('includes/footer.html');//footer
                        exit();//kill the script
                    }else{//incorrect number of rows or query has gone wrong
                        echo '<p class="error">The user cannot be altered due to a system
error.';//public message
                        //echo '<p>' . mysqli_error($dbc) . '<br />Query:' . $query .
'</p>';//debug
                    }//update or fail

                }

        }else{//display errors

                echo '<p class="error">The following errors have occurred: <br />';
                foreach($errors AS $msg){
                        echo " - $msg<br />\n";
                }
                echo '<p>Please try again.';

        }//end of empty errors IF

}//end of SUBMIT conditional

//retrieve user info using GET which is first viewing of form and page
$query = "SELECT first_name, last_name FROM customers WHERE customer_id=$id";//go get
the customer from the database
$result = mysqli_query($dbc, $query);
//var_dump($_GET); //just testing
if (mysqli_num_rows($result)==1){//valid user id show the form

        //get user info
        $row = mysqli_fetch_array ($result, MYSQLI_NUM);
        //create the form: I wouldn't allow the pin to be sticky in real life

        echo '
        <form action ="edit_customer.php" method="post">
        <p>First Name: <input type="text" name="first_name" size="15" maxlength="15" value="' .
$row['0'] . '" /></p>
        <p>Last Name:  <input type="text" name="last_name" size="15" maxlength="30"
value="' . $row['1'] . '" /></p>';?>
        <p>Current Pin: <input type="password" name="pin" size="4" maxlength="4" value="<?
php if(isset($_POST['pin'])) echo $_POST['pin']; ?>" /></p>
        <p>New Pin: <input type="password" name="pin1" size="4" maxlength="4" value="<?php
if(isset($_POST['pin1'])) echo $_POST['pin1']; ?>" /></p>
        <p>Confirm New Pin: <input type="password" name="pin2" size="4" maxlength="4"
value="<?php if(isset($_POST['pin2'])) echo $_POST['pin2']; ?>" /></p>
        <?php
        echo '
        <p><input type=submit name="submit" value="Submit" /> </p>
        <input type="hidden" name ="id" value="' . $id. '" />
        </form>
        ';
}else{//not a valid user id
echo '<p class="error">This page has been accessed in error.</p>';
```

```
}

mysqli_close($dbc);

include ('includes/footer.html');
?>
```