```php
<?php #script transfer_cash.php
//from review and pursue exercises suggested chapter 9
//this script allows a user to check their transfer cash to another account
//requires output buffering to be enabled in php: check your php core with
phpinfo();
//a bit messy and probably could be rewritten in a tidier fashion
//but time to move on as I have already stuck in techniques that haven't yet
been taught...

$page_title = 'Transfer Money';
include ('includes/header.html');

//check for form submission
if ($_SERVER['REQUEST_METHOD']=='POST'){

	require ('includes/mysqli_connect.php');//connect to the db

	$errors = array();//initialise an array for errors

	//check all account details for FROM
	//check for an entered number as pin
	if (!is_numeric($_POST['pin'])){
		$errors[] = 'You did not enter a valid pin number.';
	}else{//a number was entered: check number exists in db
		$pin1 = mysqli_real_escape_string($dbc, trim($_POST['pin']));
		$q = "SELECT AES_DECRYPT(pin,nac1) AS pin FROM customers WHERE
AES_DECRYPT(pin,nac1) = $pin1";
		$r = @mysqli_query($dbc,$q);

		$row_count = @mysqli_num_rows($r);//how many rows returned from the
query

		if ($row_count == 1){//1 row returned: match made
			$pin_num = TRUE;
		}else{//no match or too many matches
			$pin_num = FALSE;
		}

		//check for an existing pin
		if (!$pin_num){//no row found with this pin
			$errors[] = 'This pin number does not exist.';
		}else{//pin exists
			$pin = mysqli_real_escape_string($dbc, trim($_POST['pin']));
		}
	}//end of checking the pin

	//check for first name FROM
	if(empty($_POST['first_name'])){
		$errors[] = 'You did not enter your first name';
	}else{
		$fn = mysqli_real_escape_string($dbc, trim($_POST['first_name']));
	}

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

	//check for an account number FROM
	if(!is_numeric($_POST['ac_num'])){
```

```
            $errors[] = 'You did not enter a valid account number for
yourself.';
      }else{
            $ac_id = mysqli_real_escape_string($dbc, trim($_POST['ac_num']));
      }

      //check for the amount to be transferred FROM
      if(!is_numeric($_POST['amount']) || ($_POST['amount'] < 1)){//must be
positive number not zero
            $errors[] = 'You did not enter a valid amount to be transferred.';
      }else{
            $amount = mysqli_real_escape_string($dbc, trim($_POST['amount']));
            $amount = (int)$amount //whole numbers only accepted
      }

      //check details of account amount to be transferred TO
      //check for first name TO
      if(empty($_POST['first_name2'])){
            $errors[] = 'You forgot to enter a first name';
      }else{
            $fn2 = mysqli_real_escape_string($dbc, trim($_POST['first_name2']));
      }

      //check for last name TO
      if(empty($_POST['last_name2'])){
            $errors[] = 'You did not enter a last name.';
      }else{
            $ln2 = mysqli_real_escape_string($dbc, trim($_POST['last_name2']));
      }

      //check for an account number TO
      if(!is_numeric($_POST['ac_num2'])){
            $errors[] = 'You did not enter a valid account number for
transferee';
      }else{
            $ac_id2 = mysqli_real_escape_string($dbc, trim($_POST['ac_num2']));
      }

      if (empty($errors)){//all info entered and correct type

      $mistakes=array();

      //check name and account combo FROM exists
            $query = "SELECT c.first_name, c.last_name, a.account_id
                        FROM customers AS c
                        INNER JOIN accounts AS a
                        USING ( customer_id )
                        WHERE (AES_DECRYPT( pin, nac1 )) = '$pin'
                        AND c.first_name = '$fn'
                        AND c.last_name = '$ln'
                        AND a.account_id = '$ac_id'";
            $result1 = @mysqli_query($dbc, $query);
            $row_count1 = @mysqli_num_rows($result1); //how many rows returned
from the query
            //echo $row_count1;
            if ($row_count1 == 1){//1 row returned: match made
                  $from = TRUE;
            }else{//details not correct
                  $from = FALSE;
            }

            //check name and account combo TO exists
```

```
            $query2 = "SELECT c.first_name, c.last_name, a.account_id
                        FROM customers AS c
                        INNER JOIN accounts AS a
                        USING ( customer_id )
                        WHERE c.first_name = '$fn2'
                        AND c.last_name = '$ln2'
                        AND a.account_id = '$ac_id2'";
            $result2 = @mysqli_query($dbc, $query2);
            $count_row2 = @mysqli_num_rows($result2);
            //echo $count_row2;
            if ($count_row2 == 1){//1 row returned: match made
                  $to = TRUE;
            }else{//details not correct
                  $to = FALSE;
            }

            //if the above queries are OK then UPDATE the account balances
            if ($from && $to){
                  mysqli_query($dbc, "START TRANSACTION");//start sql
transaction
                  $query_from = "UPDATE accounts
                  SET balance = (balance - '$amount')
                  WHERE account_id = '$ac_id'";
                  $result_from = @mysqli_query($dbc, $query_from);

                        if (mysqli_affected_rows($dbc) == 1){//it ran OK
                              $transfer_from = TRUE;
                        }else{
                              $transfer_from = FALSE;
                              //$mistakes[] = 'This transfer from you has
failed. line139';
                        }

                  //add amount to transferee account
                  if ($transfer_from){//if the above UPDATE FROM was OK
                        $query_to = "UPDATE accounts
                        SET balance = (balance + '$amount')
                        WHERE account_id = '$ac_id2'";
                        $result_to = mysqli_query($dbc, $query_to);

                              if (mysqli_affected_rows($dbc) == 1){//if UPDATE
TO ran OK
                              $query_in = "INSERT INTO transactions
(to_account_id, from_account_id, amount)
                                                VALUES ('$ac_id2',
'$ac_id', '$amount')";
                              $result_in = @mysqli_query($dbc,$query_in);

                              mysqli_query($dbc,"COMMIT"); //complete all sql
queries

                              $URL = 'http://' . $_SERVER['HTTP_HOST'] .
dirname($_SERVER['PHP_SELF']);

                              if ((substr($url,-1) == '/') OR (substr($url, -1)
== '\\')){
                                    $url = substr ($url, 0, -1);
                              }
                              $url .='/ch9/thanks.php?ac_id=' . $ac_id //?
ac_id=$ac_id added 28.9.12
                              header("Location: $url");
                              exit();
```

```
                              }else{
                                    $mistakes[] = 'This transfer to transferee
has failed.';
                                    mysqli_query($dbc,"ROLLBACK");//undo all sql
changes
                              }
                        }else{
                              $mistakes[] = 'This transfer from you has failed';
                              mysqli_query($dbc,"ROLLBACK");//undo all sql
changes
                        }
                  }else{
                        if (!$from && !$to){
                              mysqli_query($dbc, "ROLLBACK");//undo all sql
changes
                              $mistakes[] = 'Your customer and transferee
details are not correct';
                        }elseif (!$to){
                              $mistakes[] = 'Your transferee details are not
correct';
                        }elseif(!$from ){
                              $mistakes[] = 'Incorrect customer details have
been entered';
                        }else{
                              $mistakes[] = 'Incorrect details have been
entered.';
                        }
                  }//end of if check to see if input values existis TRUE
                  //$page_title = 'Transfer Money';
                  //include ('includes/header.html');
                  echo '<h1>Mistakes!</h1>
                  <p class="error">The following mistakes occured: <br />';
                  foreach($mistakes as $msg){//print out each relevant message
                  echo " -$msg<br />\n";
                  }//print out mistakes

                  echo '<p>Please try again.</p><p><br /></p>';
                  @mysqli_close($dbc);//close conx

      }else{//errors array
            //$page_title = 'Transfer Money';
            //include ('includes/header.html');
            echo '<h1>Error!</h1>
            <p class="error">The following errors occured: <br />';
            foreach($errors as $msg){//print out each relevant message
            echo " -$msg<br />\n";
      }//print out errors

            echo '<p>Please try again.</p><p><br /></p>';

      }//end of if(empty errors)

      @mysqli_close($dbc);//close the db conx

}//end of the main Submit conditional
//$page_title = 'Transfer Money';
//include ('includes/header.html');
?>
<h1>Money Transfer</h1>
<form action="transfer_cash_header.php" method="post">
      <h3>Transfer From</h3>
```

```
      <p>Your Pin: <input type="password" name="pin" size="4" maxlength="4"
/></p>
      <p>First Name: <input type="text" name="first_name" size="15"
maxlength="20"
            value="<?php if isset $_POST['first_name']) echo
$_POST['first_name']; ?>" /></p>
      <p>Last Name: <input type="text" name="last_name" size="15" maxlength="40"
            value="<?php if isset $_POST['last_name']) echo
$_POST['last_name']; ?>" /></p>
      <p>Account Number: <input type="text" name="ac_num" size="4" maxlength="4"
            value="<?php if isset $_POST['ac_num']) echo $_POST['ac_num']; ?>"
/></p>
            <p>Amount to be Transferred <br />     (whole numbers
only): <input type="text" name="amount" size="7" maxlength="7"
                  value="<?php if isset($_POST['amount']) echo
$_POST['amount']; ?>" /></p>
      <hr/>
      <h3>Transfer To</h3>
      <p>First Name: <input type="text" name="first_name2" size="15"
maxlength="20"
            value="<?php if isset $_POST['first_name2']) echo
$_POST['first_name2']; ?>" /></p>
      <p>Last Name: <input type="text" name="last_name2" size="15"
maxlength="40"
            value="<?php if isset $_POST['last_name2']) echo
$_POST['last_name2']; ?>" /></p>
      <p>Account Number: <input type="text" name="ac_num2" size="4"
maxlength="4"
            value="<?php if isset $_POST['ac_num2']) echo $_POST['ac_num2']; ?
>" /></p>

      <p><input type="submit" name="submit" value="Transfer" /></p>
</form>
<?php include ('includes/footer.html'); ?>
```