

```

1  <?php
2  //connect to database
3  require "mysql.php";
4
5  if (!@session_start()){
6      die("Cannot start session");
7  }
8
9  if (!isset($_SESSION['valid_user'])){
10     echo '<script type="text/javascript"> alert("You must login.");';
11     echo 'window.location.replace("index.php"); </script>';
12     exit();
13 }
14 ?>
15 <html>
16 <head>
17     <title>Taste It Again - About Us</title>
18 </head>
19
20 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"gray">
21
22     <table cellspacing="0" cellpadding="0" width="900" align="center" style="border:3px
#000000 solid">
23
24         <?php include("header.php"); ?>
25
26         <tr height="500" bgcolor="white">
27             <td colspan="2">
28                 <table cellspacing="0" cellpadding="0" width="900" border="0" height=
"100%">
29                     <tr valign="top">
30                         <td>
31                             <center><h1>About Us</h1><center>
32                         </td>
33                     </tr>
34                     <tr>
35                         <td>
36                             Taste it Again, across from the Bloomfield Center redevelopment
site, was started by Jacqueline Warburton and Ivolett Bredwood,
lifelong friends from Jamaica, in time for Bloomfield's
restaurant week in early March. Try the Ackee and Saltfish
("Jamaica's National Dish" $13) and the tender Jerk Chicken
($10.50) and one of the homemade specialty drinks, like Sorrel
(made from the herb) or ginger beer.
37                         </td>
38                     </tr>
39                 </table>
40             </td>
41         </tr>
42         <tr height="30px" bgcolor="#FFFF00">
43             <td colspan="2">
44

```

```
45         <?php include("footer.php"); ?>
46
47     </td>
48 </tr>
49 </table>
50 </body>
51 </html>
52
```

```
1  <?php
2  //connect to database
3  require "mysql.php";
4
5  if (!@session_start()){
6      die("Cannot start session");
7  }
8
9  if (!isset($_SESSION['valid_user'])){
10     echo '<script type="text/javascript">'. "\n";
11     echo 'alert("You must login.");'. "\n";
12     echo 'window.location.replace("index.php");'. "\n";
13     echo '</script>'. "\n";
14     exit();
15 }
16 /*
17 echo "firstname   ".$_SESSION['firstname']."    <br/>";
18 echo "isAdmin     ".$_SESSION['isAdmin']."      <br/>";
19 echo "isOwner      ".$_SESSION['isOwner']."      <br/>";
20 echo "isCustomer   ".$_SESSION['isCustomer']."   <br/>";
21 echo "email        ".$_SESSION['email']."        <br/>";
22 */
23
24 if($_SESSION['isAdmin'] != 'Y'){
25     echo '<script type="text/javascript">'. "\n";
26     echo 'alert("Only administrators can use this page");'. "\n";
27     echo 'window.history.back();'. "\n";
28     echo '</script>'. "\n";
29     exit();
30 }
31
32 ?>
33
34 <script type="text/javascript">
35 function get_name(f)
36 {
37     f.updateFlag.value = "UPDATE";
38
39     f.fieldData.value = prompt("Please enter the new name: ",f.fieldData.value);
40
41     f.submit();
42 }
43 </script>
44
45 <html>
46 <head>
47     <title>Taste it again - Category Admin</title>
48     <?php //include("head.php"); ?>
49 </head>
50 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"black">
51     <table cellpadding="0" cellspacing="0" width="900" align="center" border="0">
52
```

```

53         <?php include("header.php"); ?>
54
55         <tr height="500" bgcolor="#82FA58">
56             <td colspan="2">
57                 <table cellpadding="0" cellspacing="0" width="900" border="0" height="
                    "100%">
58                     <tr valign="top">
59                         <td><center>
60 <!------- Start of main content
                    ----->
61 <?php
62 /*
63 echo "<pre>\n";
64 print_r($_POST);
65 echo "</pre>\n";
66 */
67
68 //operation variables are the operation being performed by admin
69 $operation = $_POST['operation']; //SQL Operation UPDATE, INSERT, or DELETE
70 if ($_POST[updateFlag] == "UPDATE")
71     $operation = "UPDATE";
72 $fieldData = $_POST['fieldData']; //data of the field being operated on
73 $fieldName = $_POST['fieldName']; //name of the field being operated on
74 $keyFieldData = $_POST['keyFieldData']; //primary key field name of the record being
operated on
75 $keyFieldName = $_POST['keyFieldName']; //primary key value of the record being
operated on
76 $table = "CATEGORIES";
77
78 /*echo"operation    $operation    <br />\n";
79 echo"keyFieldData $keyFieldData<br />\n";
80 echo"keyFieldName $keyFieldName<br />\n";
81 echo"fieldData    $fieldData    <br />\n";
82 echo"fieldName    $fieldName    <br />\n";
83 echo"table        $table        <br />\n";
84 */
85
86 if ($operation == "UPDATE" && $fieldName != "" && $keyFieldName != "" && $keyFieldData
!= "")
87 {
88     $sql="UPDATE {$table} SET {$fieldName} = '{$fieldData}' WHERE {$keyFieldName} = '
{$keyFieldData}';";
89 }else{
90     if (($operation == "Delete") && ($keyFieldName != "") && ($keyFieldData != ""))
91     {
92         $sql="DELETE FROM {$table} WHERE {$keyFieldName} = '{$keyFieldData}';";
93     }else{
94         if (($operation == "INSERT") && ($fieldName != "") && ($fieldData != ""))
95         {
96             $sql="INSERT INTO {$table} ({$fieldName}) VALUES ('{$fieldData}')";
97         }else{
98             echo "Operation or values are incorrect. <br />";
99         }

```

```

100     }
101 }
102
103 if ($sql != "")
104 {
105     //echo "<br>attempting to run query $sql" . "<br>";
106     if (!($results = $mysqli->query($sql))){
107         echo("Operation query failed.<br />");
108         echo("sql: $sql<br />");
109     }
110 }
111
112 // Get whole table
113 $sql = "SELECT * from {$table}";
114 if (!($results = $mysqli->query($sql))){
115     die("Query to show fields from table failed: $sql");
116 }
117 echo "<h1>Edit Table: {$table}</h1>";
118 echo 'You are logged in as: '.$_SESSION['valid_user'].'<br/>';
119 echo "\n".<table>';
120 echo "\n".<form action="'.$_SERVER['SCRIPT_NAME'].' " method="POST" >';
121 echo "\n".<tr><td>Enter a new Category Name: </td><td><input type="text"
name="fieldData" value="" ></td></tr>';
122 echo "\n".<input type="hidden" name="operation" value="INSERT">';
123 echo "\n".<input type="hidden" name="fieldName" value="NAME">';
124 echo "\n".<tr><td align="center" colspan = "2"><input type="submit" value="Add
Category" >';
125 echo "\n".</form>';
126 echo "\n".</table>';
127
128 echo '<table style="border:1px #000000 solid" bgcolor="white"><tr>';
129 $finfo = $results->fetch_fields();
130 foreach ($finfo as $val) {
131     echo "<td>{$val->name}</td>";
132 }
133 echo "</tr>\n";
134
135 // printing table rows
136 while($row = $results->fetch_row())
137 {
138     echo "<tr>";
139
140     //test comment
141     foreach($row as $cell)
142     echo "<td>{$cell}</td>";
143     echo "\n".<form action="'.$_SERVER['SCRIPT_NAME'].' " method="POST">'. "\n";
144     echo '<td><input type="button" name="btnChangeName" value="ChangeName"
onclick="get_name(this.form);"></td>'. "\n";
145     echo '<td><input type="submit" name="operation" value="Delete"
> </td>'. "\n";
146     echo ' <input type="hidden" name="keyFieldData" value="'.$row[0].
' " >'. "\n"; //the key value of the record being
operated on

```

```

147     echo '      <input type="hidden" name="keyFieldName" value="'. $finfo[0] -> name.
        ' "
        >'. "\n" ; //the name of the key field
148     echo '      <input type="hidden" name="fieldName" value="'. $finfo[1] -> name.
        ' "
        >'. "\n" ; //the name of the field being updated
149     echo '      <input type="hidden" name="fieldData" value="'. $row[1].
        ' "
        >'. "\n" ; //holds the new name, set in get_name
150     echo '      <input type="hidden" name="updateFlag"
        value=""
        >'. "\n" ; //holds the new name,
        set in get_name
151     echo "</form>";
152     echo "</tr>\n";
153 }
154 echo "</table>";
155
156 $results->close();
157 ?>
158
159
160 <!-- End
-----
----->

161         </td>
162     </tr>
163 </table>
164 </td>
165 </tr>
166 <tr height="30px" bgcolor="#FFFF00">
167     <td colspan="2">
168
169         <?php include( "footer.php" ); ?>
170
171     </td>
172 </tr>
173 </table>
174 </body>
175
176 </html>

```

```
1  <?php
2  if (!@session_start()){
3      die("Cannot start session");
4  }
5
6  //check if in a valid session
7  if (!isset($_SESSION['valid_user'])){
8      //they have not tried to login, or logged out
9      echo '<script type="text/javascript">';
10     echo 'alert("You must login first");';
11     echo 'window.location.replace("index.php");';
12     echo '</script>';
13     exit();
14 }
15
16 $referer = $_SERVER['HTTP_REFERER'];
17 //check if is a customer
18 if ($_SESSION['isCustomer'] != 'Y'){
19     echo '<script type="text/javascript"> ';
20     echo 'alert("You must login or create an account before you can checkout.");';
21     echo "window.location.replace(\"$referer\")";
22     echo '</script>';
23     exit();
24 }
25
26 //check if any items in cart
27 if (count($_SESSION['cart']) == 0){
28     echo '<script type="text/javascript"> ';
29     echo 'alert("Your cart is empty");';
30     echo "window.location.replace(\"$referer\")";
31     echo '</script>';
32     exit();
33 }
34
35 $cart = $_SESSION['cart'];
36
37 ?>
38
39 <html>
40 <head>
41     <title>Taste It Again - Check Out</title>
42 </head>
43 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"black">
44 <script type="text/javascript">
45 <!--
46 function test_it(f){
47     if(f.checkValidity()){
48         f.posted.value = "OK";
49         f.submit();
50     }
51     else{
52         alert("Please check all fields for valid data");
```

```
53         return ;
54     }
55 }
56 //-->
57 </script>
58
59 <?php
60 require "mysql.php";
61
62 /*echo '<pre>';
63 print_r($_POST);
64 echo '</pre>';*/
65
66 $posted    = $_POST['posted'];
67
68 if($posted == "OK"){
69     //user attempted checkout
70     $userid    = $_POST['userid'];
71     $fName     = $_POST['fName'];
72     $lName     = $_POST['lName'];
73     $address   = $_POST['address'];
74     $address2  = $_POST['address2'];
75     $city      = $_POST['city'];
76     $state     = $_POST['state'];
77     $zipCode   = $_POST['zipCode'];
78     $newemail  = $_POST['email'];
79     $phone     = $_POST['phone'];
80     $txtflag   = $_POST['txtflag'];
81     $mailflag  = $_POST['mailflag'];
82 }else{
83     $email = $_SESSION['email'];
84     //load account info from database
85     //get USER record
86     $sql = "select * from USERS where EMAILADD = '$email'";
87     //echo "sql: $sql<br />";
88     if (!($results = $mysqli->query($sql))){
89         die("Cannot get USER record: ".$mysqli->error);
90     }
91     if ($results->num_rows != 1){
92         die("USERS - Wrong number of rows: ".$results->num_rows."      $sql");
93     }
94     $row = $results->fetch_assoc();
95     $userid = $row['USERID'];
96     $fName  = $row['FIRSTNAME'];
97     $lName  = $row['LASTNAME'];
98     $phone  = $row['PHONE'];
99
100     //get CUSTOMER record
101     $sql = "select * from CUSTOMERS where USERID = '$userid'";
102     if (!($results = $mysqli->query($sql))){
103         die("Cannot get CUSTOMER record: ".$mysqli->error);
104     }
105     if ($results->num_rows != 1){
```



```

106         die("CUSTOMERS - Wrong number of rows: ".$results->num_rows);
107     }
108     $row = $results->fetch_assoc();
109     $address = $row['ADDLINE1'];
110     $address2 = $row['ADDLINE2'];
111     $city = $row['CITY'];
112     $state = $row['STATE'];
113     $zipCode = $row['ZIP'];
114     $mailflag = $row['EMAILFLAG'];
115     $txtflag = $row['TXTMSGFLAG'];
116 }
117
118 if ($posted == "OK"){
119     //insert new order
120     $ordUID = uniqid(); //create unique ID
121     $fullName = $fName." ".$lName;
122     $time = date("Y-m-d H:i:s", time());
123
124     $sql1 = "INSERT INTO `ORDERS`
125             (`ORDID`, `CUSTID`, `FULLNAME`, `CONTACTPHONE`, `DELIVERFLAG`,
126             `DELADDLINE1`, `DELADDLINE2`, `DELCITY`, `DELSTATE`, `DELZIP`, `TIME`)
127             VALUES ('$ordUID', '$userid', '$fullName', '$phone', 'TRUE', '$address',
128             '$address2', '$city', '$state', '$zipCode', '$time')";
129
130     //transaction begin with implicit autocommit off
131     if (!$mysqli->query("START TRANSACTION;")){
132         echo '<script type="text/javascript">'. "\n";
133         echo 'alert("Start transaction failed: '.$mysqli->error.'");'. "\n";
134         echo 'window.back();';
135         echo '</script>'. "\n";
136         exit();
137     }
138
139     //insert into ORDERS table
140     if (!$mysqli->query($sql1)){
141         //rollback
142         $err = $mysqli->error; //save error message before rollback
143         $mysqli->query("ROLLBACK;"); //must add check for rollback failure
144         echo '<script type="text/javascript">'. "\n";
145         echo 'alert("Account update failed: '.$err.'");'. "\n";
146         echo 'window.back();';
147         echo '</script>'. "\n";
148         exit();
149     }
150
151     //insert ORDERITEMS information
152     $lineNum = 0;
153     foreach($cart as $key=>$value){
154         ++$lineNum;
155         $sql2 = "insert into `ORDERITEMS`
156                 (`ORDID`,

```

```

157         `EXTPRICE`,
158         `NAME`,
159         `PRICE`,
160         `TAXABLE`)
161     select
162         '$ordUID' as ORDID,
163         '$lineNum' as LINENUM,
164         '$value' as QTY,
165         ($value * PRICE) as EXTPRICE,
166         NAME,
167         PRICE,
168         TAXABLE
169     from PRODUCTS
170     where PRODID = '$key';
171
172     echo '<script type="text/javascript">'. "\n";
173     echo 'alert('.$sql2. ');'. "\n";
174     echo 'window.back();';
175     echo '</script>'. "\n";
176
177     if (!$mysqli->query($sql2)){
178         $err = $mysqli->error; //save error message before rollback
179         //rollback
180         $mysqli->query("ROLLBACK;"); //must add check for rollback failure
181         echo '<script type="text/javascript">'. "\n";
182         echo 'alert("Account update failed: '.$err.'");'. "\n";
183         echo 'window.back();';
184         echo '</script>'. "\n";
185         exit();
186     }
187 } //end foreach
188
189 if (($lineNum > 0) && ($lineNum == count($cart))){ //make sure all line items were
added
190     //commit transaction
191     if ($mysqli->query("COMMIT;")){
192         unset($cart);
193         unset($_SESSION['cart']);
194         echo '<script type="text/javascript">'. "\n";
195         echo 'alert("Order Saved, confirmation sent to '.$_SESSION['email'].'");'.
"\n";
196         echo 'window.location.replace("displayorder.php?ordUID='.$ordUID.'");';
197         echo '</script>'. "\n";
198     }else{
199         echo '<script type="text/javascript">'. "\n";
200         echo 'alert("Commit transaction failed: '.$mysqli->error.'");'. "\n";
201         echo 'window.back();';
202         echo '</script>'. "\n";
203         exit();
204     }
205 }else{
206     //rollback
207     $mysqli->query("ROLLBACK;"); //must add check for rollback failure

```

```

208     echo '<script type="text/javascript">'. "\n";
209     echo 'alert("Account update failed: '.$serr.'");'. "\n";
210     echo 'window.back();';
211     echo '</script>'. "\n";
212     exit();
213 }
214 }
215 ?>
216
217 <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">
218
219     <?php include("header.php"); ?>
220
221     <tr height="500" bgcolor="#82FA58">
222         <td colspan="2">
223             <table cellspacing="0" cellpadding="0" width="900" border="0" height=
224                 "100%">
225                 <tr valign="top">
226                     <td>
227                         <table cellspacing="0" cellpadding="0" width="900" border=
228                             "0">
229                             <tr>
230                                 <td>
231                                     <center><h1>Checkout</h1></center>
232                                 </td>
233                             </tr>
234                         </table>
235                         <form name="update" id="update" action = '' method = "post">
236                         <table cellspacing="1" cellpadding="3" style="border:1px
237                             #000000 solid" bgcolor="#BDBDBD" align="center">
238                             <tr>
239                                 <td colspan="2" align="center">
240                                     <b><ul>Update Delivery Address</ul></b>
241                                 </td>
242                             </tr>
243                             <tr>
244                                 <td>
245                                     First Name
246                                 </td>
247                                 <td>
248                                     <input type="text"
249                                         name="fName"
250                                         required
251                                         size="20"
252                                         value="<?php echo $fName; ?>"
253                                 </td>
254                             </tr>
255                             <tr>
256                                 <td>
257                                     Last Name
258                                 </td>
259                                 <td>
260                                     <input type="text"

```

```
258         name="lName"
259         required
260         size="20"
261         value="php echo $lName; ?">
262     </td>
263 </tr>
264 <tr>
265     <td>
266         Address
267     </td>
268     <td>
269         <input type="text"
270         name="address"
271         required
272         size="20"
273         value="php echo $address; ?">
274     </td>
275 </tr>
276 <tr>
277     <td>
278         Address Line 2
279     </td>
280     <td>
281         <input type="text"
282         name="address2"
283         size="20"
284         value="php echo $address2; ?">
285     </td>
286 </tr>
287 <tr>
288     <td>
289         City
290     </td>
291     <td>
292         <input type="text"
293         name="city"
294         required
295         size="20"
296         value="php echo $city; ?">
297     </td>
298 </tr>
299 <tr>
300     <td>
301         State
302         <input type="text"
303         name="state"
304         size="3"
305         value="php echo $state; ?">
306     </td>
307     <td>
308         Zip Code
309         <input type="text"
310         name="zipCode"
```

```

311         required
312         size="5"
313         value="<?php echo $zipCode; ?>"
314     </td>
315 </tr>
316 <tr>
317     <td>
318         Phone Number
319     </td>
320     <td>
321         <input type="text"
322             name="phone"
323             required
324             size="20"
325             value="<?php echo $phone; ?>"
326         </td>
327 </tr>
328 <tr>
329     <td>
330         Email Address
331     </td>
332     <td>
333         <input type="text"
334             name="email" size="30"
335             required
336             value="<?php echo $email; ?>"
337         </td>
338 </tr>
339 <tr>
340     <td>
341         Credit Card Number
342     </td>
343     <td>
344         <input type="text"
345             name="ccnum" size="30"
346             required
347             pattern="[A-Z]|[a-z]{16}"
348             title="for this demonstration system, input 16
349             letters"
350             maxlength="16"
351             length
352             value=""
353         </td>
354 </tr>
355 </table>
356 <table align="center">
357     <tr>
358     <td>
359         <input name="btnSave" type="button" value=
360             "Checkout" onclick="test_it(this.form);"/>
361         <!--<input type="reset" value="Reset">-->
362     </td>

```

```
362         </tr>
363     </table>
364     <input name="posted" type="hidden" value="">
365     <input name="userid" type="hidden" value=<?php echo $userid;
366         ?>>
367     </form>
368 </td>
369 </tr>
370 </table>
371 </td>
372 </tr>
373 <tr height="30px" bgcolor="#FFFF00">
374     <td colspan="2">
375         <?php include("footer.php"); ?>
376     </td>
377 </tr>
378 </table>
379 </body>
380 </html>
381
382
```

```
1  <?php
2  if (!@session_start()){
3      die("Cannot start session");
4  }
5
6  //check if in a valid session
7  if (!isset($_SESSION['valid_user'])){
8      //they have not tried to login, or logged out
9      echo '<script type="text/javascript">';
10     echo 'alert("You must login first");';
11     echo 'window.location.replace("index.php");';
12     echo '</script>';
13     exit();
14 }
15
16 //check if is a customer
17 if ($_SESSION['isCustomer'] != 'Y'){
18     echo '<script type="text/javascript"> ';
19     echo 'alert("You must logged in to view your order.");';
20     echo '</script>';
21     echo 'window.location = ".".$_SERVER["HTTP_REFERER"]."';
22     exit();
23 }
24
25 $ordUID = $_GET['ordUID'];
26 ?>
27
28 <html>
29 <head>
30     <title>Taste It Again - Check Out</title>
31 </head>
32 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"black">
33 <script type="text/javascript">
34 <!--
35 function test_it(f){
36     if(f.checkValidity()){
37         f.posted.value = "OK";
38         f.submit();
39     }
40     else{
41         alert("Please check all fields for valid data");
42         return ;
43     }
44 }
45 //-->
46 </script>
47
48 <?php
49 require "mysql.php";
50
51 /*echo '<pre>';
52 print_r($_POST);
```

```

53  echo '</pre>';*/
54
55  $posted    = $_POST['posted'];
56
57  if($posted == "OK"){
58      //user attempted checkout
59      $userid    = $_POST['userid'];
60      $fName     = $_POST['fName'];
61      $lName     = $_POST['lName'];
62      $address   = $_POST['address'];
63      $address2  = $_POST['address2'];
64      $city      = $_POST['city'];
65      $state     = $_POST['state'];
66      $zipCode   = $_POST['zipCode'];
67      $newemail  = $_POST['email'];
68      $phone     = $_POST['phone'];
69      $txtflag   = $_POST['txtflag'];
70      $mailflag  = $_POST['mailflag'];
71  }else{
72      $email = $_SESSION['email'];
73      //load account info from database
74      //get USER record
75      $sql = "select * from USERS where EMAILADD = '$email'";
76      //echo "sql: $sql<br />";
77      if (!($results = $mysqli->query($sql))){
78          die("Cannot get USER record: ".$mysqli->error);
79      }
80      if ($results->num_rows != 1){
81          die("USERS - Wrong number of rows: ".$results->num_rows."      $sql");
82      }
83      $row = $results->fetch_assoc();
84      $userid = $row['USERID'];
85      $fName  = $row['FIRSTNAME'];
86      $lName  = $row['LASTNAME'];
87      $phone  = $row['PHONE'];
88
89      //get CUSTOMER record
90      $sql = "select * from CUSTOMERS where USERID = '$userid'";
91      if (!($results = $mysqli->query($sql))){
92          die("Cannot get CUSTOMER record: ".$mysqli->error);
93      }
94      if ($results->num_rows != 1){
95          die("CUSTOMERS - Wrong number of rows: ".$results->num_rows);
96      }
97      $row = $results->fetch_assoc();
98      $address = $row['ADDLINE1'];
99      $address2 = $row['ADDLINE2'];
100     $city     = $row['CITY'];
101     $state    = $row['STATE'];
102     $zipCode  = $row['ZIP'];
103     $mailflag = $row['EMAILFLAG'];
104     $txtflag  = $row['TXTMSGFLAG'];
105 }

```



```

106
107 if ($posted == "OK"){
108     //insert new order
109     $ordUID = uniqid(); //create unique ID
110     $fullName = $fName." ".$lName;
111     $time = time();
112
113     $sql1 = "INSERT INTO `ORDERS`
114             (`ORDID` , `CUSTID` , `FULLNAME` , `CONTACTPHONE` , `DELIVERFLAG` ,
115             `DELADDLINE1` , `DELADDLINE2` , `DELCITY` , `DELSTATE` , `DELZIP` , `TIME`)
116     VALUES ('$ordUID' , '$userid' , '$fullName' , '$phone' , 'TRUE' , '$address
117             ' , '$address2' , '$city' , '$state' , '$zipCode' , $time)";
118
119     //transaction begin with implicit autocommit off
120     if (!$mysqli->query("START TRANSACTION;")){
121         echo '<script type="text/javascript">'. "\n";
122         echo 'alert("Start transaction failed: '.$mysqli->error.'");'. "\n";
123         echo 'window.back();';
124         echo '</script>'. "\n";
125         exit();
126     }
127
128     //insert into ORDERS table
129     if (!$mysqli->query($sql1)){
130         //rollback
131         $err = $mysqli->error; //save error message before rollback
132         $mysqli->query("ROLLBACK;"); //must add check for rollback failure
133         echo '<script type="text/javascript">'. "\n";
134         echo 'alert("Account update failed: '.$err.'");'. "\n";
135         echo 'window.back();';
136         echo '</script>'. "\n";
137         exit();
138     }
139
140     //insert ORDERITEMS information
141     $lineNum = 0;
142     foreach($cart as $key=>$value){
143         echo "in loop<br />";
144         ++$lineNum;
145         $sql2 = "insert into `ORDERITEMS`
146                 (`ORDID` ,
147                 `LINENUM` ,
148                 `QTY` ,
149                 `EXTPRICE` ,
150                 `NAME` ,
151                 `PRICE` ,
152                 `TAXABLE`)
153     select
154         '$ordUID' as ORDID,
155         '$lineNum' as LINENUM,
156         '$value' as QTY,
157         ($value * PRICE) as EXTPRICE,
158         NAME,

```

```

157         PRICE,
158         TAXABLE
159     from PRODUCTS
160     where PRODID = '$key';
161
162     echo '<script type="text/javascript">'. "\n";
163     echo 'alert('.$sql2. ');'. "\n";
164     echo 'window.back();';
165     echo '</script>'. "\n";
166
167     if (!$mysqli->query($sql2)){
168         $err = $mysqli->error; //save error message before rollback
169         //rollback
170         $mysqli->query("ROLLBACK;"); //must add check for rollback failure
171         echo '<script type="text/javascript">'. "\n";
172         echo 'alert("Account update failed: '.$err. ');'. "\n";
173         echo 'window.back();';
174         echo '</script>'. "\n";
175         exit();
176     }
177 } //end foreach
178
179 if (($lineNum > 0) && ($lineNum == count($cart))){ //make sure all line items were
    added
180     //commit transaction
181     if ($mysqli->query("COMMIT;")){
182         echo '<script type="text/javascript">'. "\n";
183         echo 'alert("Order Saved, confirmation sent to '.$_SESSION['email']. ');'.
            "\n";
184         echo 'window.location.replace("confrimorder.php");';
185         echo '</script>'. "\n";
186     }else{
187         echo '<script type="text/javascript">'. "\n";
188         echo 'alert("Commit transaction failed: '.$mysqli->error. ');'. "\n";
189         echo 'window.back();';
190         echo '</script>'. "\n";
191         exit();
192     }
193 }else{
194     //rollback
195     $mysqli->query("ROLLBACK;"); //must add check for rollback failure
196     echo '<script type="text/javascript">'. "\n";
197     echo 'alert("Account update failed: '.$err. ');'. "\n";
198     echo 'window.back();';
199     echo '</script>'. "\n";
200     exit();
201 }
202 }
203 ?>
204
205 <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">
206
207     <?php include("header.php"); ?>

```

```

208
209     <tr height="500" bgcolor="#82FA58">
210         <td colspan="2">
211             <table cellspacing="0" cellpadding="0" width="900" border="0" height=
212                 "100%">
213                 <tr valign="top">
214                     <td>
215                         <table cellspacing="0" cellpadding="0" width="900" border=
216                             "0">
217                             <tr>
218                                 <td>
219                                     <center><h1>Checkout</h1></center>
220                                 </td>
221                             </tr>
222                         </table>
223                         <form name="update" id="update" action = '' method = "post">
224                         <table cellspacing="1" cellpadding="3" style="border:1px
225                             #000000 solid" bgcolor="#BDBDBD" align="center">
226                             <tr>
227                                 <td colspan="2" align="center">
228                                     <b><ul>Update Delivery Address</b></ul>
229                                 </td>
230                             </tr>
231                             <tr>
232                                 <td>
233                                     <b>First Name
234                                 </td>
235                                 <td>
236                                     <input type="text"
237                                         name="fName"
238                                         required
239                                         size="20"
240                                         value="<?php echo $fName; ?>"
241                                 </td>
242                             </tr>
243                             <tr>
244                                 <td>
245                                     <b>Last Name
246                                 </td>
247                                 <td>
248                                     <input type="text"
249                                         name="lName"
250                                         required
251                                         size="20"
252                                         value="<?php echo $lName; ?>"
253                                 </td>
254                             </tr>
255                             <tr>
256                                 <td>
257                                     <b>Address
258                                 </td>
259                                 <td>
260                                     <input type="text"

```

```
258         name="address"
259         required
260         size="20"
261         value="php echo $address; ?">
262     </td>
263 </tr>
264 <tr>
265     <td>
266         Address Line 2
267     </td>
268     <td>
269         <input type="text"
270         name="address2"
271         size="20"
272         value="php echo $address2; ?">
273     </td>
274 </tr>
275 <tr>
276     <td>
277         City
278     </td>
279     <td>
280         <input type="text"
281         name="city"
282         required
283         size="20"
284         value="php echo $city; ?">
285     </td>
286 </tr>
287 <tr>
288     <td>
289         State
290         <input type="text"
291         name="state"
292         size="3"
293         value="php echo $state; ?">
294     </td>
295     <td>
296         Zip Code
297         <input type="text"
298         name="zipCode"
299         required
300         size="5"
301         value="php echo $zipCode; ?">
302     </td>
303 </tr>
304 <tr>
305     <td>
306         Phone Number
307     </td>
308     <td>
309         <input type="text"
310         name="phone"
```

```

311         required
312         size="20"
313         value="<?php echo $phone; ?>"
314     </td>
315 </tr>
316 <tr>
317     <td>
318         Email Address
319     </td>
320     <td>
321         <input type="text"
322         name="email" size="30"
323         required
324         value="<?php echo $email; ?>"
325     </td>
326 </tr>
327 <tr>
328     <td>
329         Credit Card Number
330     </td>
331     <td>
332         <input type="text"
333         name="ccnum" size="30"
334         required
335         pattern="[A-Z]|[a-z]{16}"
336         title="for this demonstration system, input 16
337         letters"
338         maxlength="16"
339         length
340         value=""
341     </td>
342 </tr>
343 </table>
344 <table align="center">
345     <tr>
346         <td>
347             <input name="btnSave" type="button" value=
348             "Checkout" onclick="test_it(this.form);"/>
349             <!--<input type="reset" value="Reset">-->
350         </td>
351     </tr>
352 </table>
353 <input name="posted" type="hidden" value="">
354 <input name="userid" type="hidden" value="<?php echo $userid;
355     ?>"
356 </form>
357 </td>
358 </tr>
359 </table>
360 <tr height="30px" bgcolor="#FFFF00">

```

```
361         <td colspan="2">
362
363         <?php include( "footer.php" ); ?>
364
365     </td>
366 </tr>
367 </table>
368 </body>
369 </html>
370
```

```
1  <?php
2  //connect to database
3  require "mySQL.php";
4
5  if (!@session_start()){
6      die("Cannot start session");
7  }
8
9  if (!isset($_SESSION['valid_user'])){
10     echo '<script type="text/javascript"> alert("You must login.");';
11     echo 'window.location.replace("index.php"); </script>';
12     exit();
13 }
14 ?>
15 <html>
16 <head>
17     <title>Taste It Again - Contact Info</title>
18 </head>
19
20 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"gray">
21
22     <table cellspacing="0" cellpadding="0" width="900" align="center" style="border:3px
#000000 solid">
23
24         <?php include("header.php"); ?>
25
26         <tr height="500" bgcolor="white">
27             <td colspan="2">
28                 <table cellspacing="0" cellpadding="0" width="900" border="0" height=
"100%">
29                     <tr valign="top">
30                         <td>
31                             <center><h1>Contact Us</h1><center>
32                         </td>
33                     </tr>
34                 </table>
35             </td>
36         </tr>
37         <tr height="30px" bgcolor="#FFFF00">
38             <td colspan="2">
39
40                 <?php include("footer.php"); ?>
41
42             </td>
43         </tr>
44     </table>
45 </body>
46 </html>
47
```

```

1  <?php
2  //connect to database
3  require "mysql.php";
4
5  //based on listing 23.4 in PHP book
6  if (!@session_start()){
7      die("Cannot start session");
8  }
9
10 if (isset($_POST['u_id']) && isset($_POST['u_pwd'])){
11     //user has just tried to log in
12     $u_id = $_POST['u_id'];
13     $u_pwd = $_POST['u_pwd'];
14
15
16     $query = "select * from CPANELUSERS where USERID = '$u_id' and PWHASH = '".md5(
17         $u_pwd)."'";
18     $result = $mysqli->query($query);
19     if ($result->num_rows){
20         //if they are in the dataabse, register the user id and privileges
21         $_SESSION['valid_user'] = $u_id;
22         $row = $result->fetch_assoc();
23         $_SESSION['cpanel_admin'] = $row['ADMINFLAG'];
24         $result->close();
25     }
26     else{
27         unset($_SESSION['valid_user']);
28         unset($_SESSION['cpanel_admin']);
29         echo '<script type="text/javascript"> alert("Invalid username/password");';
30         echo 'window.history.back(); </script>';
31         exit();
32     }
33 }
34
35 <html><head>
36 <title>Edit CPanel Users</title>
37 </head>
38
39 <body>
40 <script type="text/javascript" >
41
42 function get_pw(f)
43 {
44     f.op_ChangePW.value = "ChangePW";
45
46     if (f.operation_id.value == "")
47     {
48         alert("Error - no user account selected.");
49         return;
50     }
51
52     f.operation_pwd.value = prompt("Please enter the new password: ", "");

```



```
53
54     if (f.operation_pwd.value != prompt("Please re-enter the new password: ",""))
55     {
56         alert("Passwords do not match.");
57         return;
58     }
59
60     f.submit();
61 }
62 </script>
63
64 <script type="text/javascript" >
65 function test_it(f)
66 {
67     if (f.operation_id.value == "" || f.operation_pwd.value == "")
68     {
69         alert("You have to enter a user ID and password!");
70         return;
71     }
72
73     if (f.operation_pwd.value != f.operation_pwd2.value)
74     {
75         alert("Passwords do not match");
76         return;
77     }
78
79     //changes to catch XSS and SQL injection
80     if ((f.operation_id.value.indexOf("<") != -1) || (f.operation_pwd.value.indexOf("<")
81         != -1) ||
82         (f.operation_id.value.indexOf("'") != -1) || (f.operation_pwd.value.indexOf("'") !=
83         -1))
84     {
85         alert("You have illegal characters in user ID or password!");
86         return;
87     }
88
89     //alert(f.operation_id.value + ' ' + f.operation_pwd.value );
90     f.submit();
91 }
92 </script>
93 <?php
94     if (isset($_SESSION['valid_user'])){
95         //echo 'You are logged in as: ' . $_SESSION['valid_user'] . '<br/>';
96         //echo '<a href="cPanelLogout.php">Log out</a><br />';
97     }else{
98         if(isset($u_id)){
99             //they tied and failed to login
100             echo '<script type="text/javascript"> alert("Invalid username/password");';
101             echo 'window.history.back(); </script>';
102         }else{
103             //they have not tried to login, or logged out
```

```

104     echo '<script type="text/javascript"> alert("You must login first");';
105     echo 'window.location.replace("index.php"); </script>';
106     exit();
107 }
108 }
109
110 ?>
111
112 <?php
113
114 //operation variables are the operation being performed by cpanel admin
115 $op_NewUser      = ($_POST['op_NewUser'] == "NewUser") ? "TRUE" : "FALSE";
116 $op_ChangePW     = ($_POST['op_ChangePW'] == "ChangePW") ? "TRUE" : "FALSE";
117 $op_AdminOn      = ($_POST['op_AdminOn'] == "AdminOn") ? "TRUE" : "FALSE";
118 $op_AdminOff     = ($_POST['op_AdminOff'] == "AdminOff") ? "TRUE" : "FALSE";
119 $op_Delete       = ($_POST['op_Delete'] == "Delete") ? "TRUE" : "FALSE";
120 $operation_id    = $_POST['operation_id'];
121 $operation_pwd   = $_POST['operation_pwd'];
122 $operation_hash  = md5($operation_pwd);
123 $operation_admin = empty($_POST['operation_admin']) ? 'FALSE' : $_POST['operation_admin'];
124 $table          = "CPANELUSERS";
125
126 if (!($_SESSION['cpanel_admin']=='1')){
127     echo '<script type="text/javascript"> window.location.replace("home.php") </script>';
128     exit;
129 }
130
131 if ($op_ChangePW == "TRUE" && $operation_id != "")
132 {
133     $sql="UPDATE {$table} SET PWHASH = '{$operation_hash}' WHERE USERID = '{$operation_id}';";
134 }
135
136 if ($op_Delete == "TRUE" && $operation_id != "")
137 {
138     $sql="DELETE FROM {$table} WHERE USERID = '{$operation_id}';";
139 }
140
141 if ($op_AdminOn == "TRUE" && $operation_id != "")
142 {
143     $sql="UPDATE {$table} SET ADMINFLAG = TRUE WHERE USERID = '{$operation_id}';";
144 }
145
146 if ($op_AdminOff == "TRUE" && $operation_id != "")
147 {
148     $sql="UPDATE {$table} SET ADMINFLAG = FALSE WHERE USERID = '{$operation_id}';";
149 }
150
151 if ($op_NewUser == "TRUE" && $operation_id != "" && $operation_hash != "" )
152 {
153     $sql="INSERT INTO {$table} VALUES ('{$operation_id}', '{$operation_hash}',
        {$operation_admin});";

```

```

154     }
155
156     if ($sql != "")
157     {
158         //echo "<br>attempting to run query $sql" . "<br>";
159         if (!($results = $mysqli->query($sql))){
160             echo("Operation query failed.");
161         }
162     }
163
164     // sending query
165     $sql = "SELECT * from {$table}";
166     if (!($results = $mysqli->query($sql))){
167         die("Query to show fields from table failed: $sql");
168     }
169     echo "<h1>Edit Table: {$table}</h1>";
170     echo 'You are logged in as: ' . $_SESSION['valid_user'] . "<br/>";
171     echo "\n" . "<table>";
172     echo "\n" . "<form action=\"" . $_SERVER['SCRIPT_NAME'] . "\" method=\"POST\" >";
173     echo "\n" . "<tr><td>Enter a new userID: </td><td><input type=\"text\" name=\"operation_id\"
value=\"\" ></td></tr>";
174     echo "\n" . "<tr><td>Enter a password: </td><td><input type=\"password\"
name=\"operation_pwd\" value=\"\"></td></tr>";
175     echo "\n" . "<tr><td>Re-enter password: </td><td><input type=\"password\"
name=\"operation_pwd2\" value=\"\"></td></tr>";
176     echo "\n" . "<tr><td colspan = \"2\">Admin?";
177     echo "\n" . "<input type=\"radio\" name=\"operation_admin\" value=\"TRUE\"> Y";
178     echo "\n" . "<input type=\"radio\" name=\"operation_admin\" value=\"FALSE\" checked>
N</td></tr>";
179     echo "\n" . "<input type=\"hidden\" name=\"op_NewUser\" value=\"NewUser\">";
180     echo "\n" . "<tr><td colspan = \"2\"><input type=\"button\" value=\"Add ID\"
onclick=\"test_it(this.form);\" >";
181     echo "\n" . "<input type=\"button\" value=\"Homepage\" onclick=\"location.href='\" . \"'home.php\" .
'\" >";
182     echo "\n" . "<input type=\"button\" value=\"Logout\" onclick=\"location.href='\" .
'\"cPanelLogout.php\" . \"' >";
183     echo "\n" . "<input type=\"button\" value=\"View Development Log\" onclick=\"window.open('\" .
'\"http://blue.cs.montclair.edu/~cmpt483a/dev/~DevLog.txt\" . \"')\" >";
184     echo "</td></tr>";
185     echo "\n" . "</form>";
186     echo "\n" . "</table>";
187
188     echo "<table border='1'><tr>";
189     $finfo = $results->fetch_fields();
190     foreach ($finfo as $val) {
191         echo "<td>{$val->name}</td>";
192     }
193     echo "</tr>\n";
194
195     // printing table rows
196     while($row = $results->fetch_row())
197     {
198         echo "<tr>";

```

```
199
200     //test comment
201     foreach($row as $cell)
202     echo "<td>$cell</td>";
203     echo "\n". '<form action="'. $_SERVER['SCRIPT_NAME']. ' " method="POST">'. "\n";
204     echo ' <td><input type="button" name="btnChangePW" value="ChangePW"
onclick="get_pw(this.form);"></td>'. "\n";
205     echo ' <td><input type="submit" name="op_AdminOn" value="AdminOn" ></td>'. "\n";
206     echo ' <td><input type="submit" name="op_AdminOff" value="AdminOff"></td>'. "\n";
207     echo ' <td><input type="submit" name="op_Delete" value="Delete" ></td>'. "\n";
208     echo ' <input type="hidden" name="op_ChangePW" value="" >'. "\n";
//the flag for changing password
209     echo ' <input type="hidden" name="operation_id" value="'. $row[0]. ' " >'. "\n";
//the user id being operated on
210     echo ' <input type="hidden" name="operation_pwd" value="FALSE" >'. "\n";
//holds the new password, set in get_pw
211     echo "</form>";
212     echo "</tr>\n";
213 }
214 echo "</table>";
215
216 $results->close();
217 ?>
218
219
220
221 </body></html>
```

```
1  <?php
2  session_start();
3  $old_user = $_SESSION['valid_user'];
4  unset($_SESSION['valid_user']);
5  session_destroy();
6  echo '<script type="text/javascript"> alert("You have been logged out.");';
7  echo 'window.location.replace("index.php"); </script>';
8  exit();
9  ?>
```

```

1  <?php
2  if (!@session_start()){
3      die("Cannot start session");
4  }
5
6  //check if in a valid session
7  if (!isset($_SESSION['valid_user'])){
8      //they have not tried to login, or logged out
9      echo '<script type="text/javascript">';
10     echo 'alert("You must login first");';
11     echo 'window.location.replace("index.php");';
12     echo '</script>';
13     exit();
14 }
15
16 //check if is a customer
17 if (($SESSION['isCustomer'] != 'Y') && ($SESSION['isOwner'] != 'Y')){
18     echo '<script type="text/javascript"> ';
19     echo 'alert("You must logged in as customer or owner to view orders.");';
20     echo 'window.location = "'.$_SERVER['HTTP_REFERER'].'"';
21     echo '</script>';
22     exit();
23 }
24
25 $ordUID = $_GET['ordUID'];
26 if ($ordUID == ''){
27     echo '<script type="text/javascript"> ';
28     echo 'alert("Error - invalid order ID: '.$ordUID.'");';
29     echo 'window.location = "'.$_SERVER['HTTP_REFERER'].'"';
30     echo '</script>';
31     exit();
32 }
33
34 //changes function of button at the bottom
35 $calledBy = $_GET['calledBy'];
36
37 ?>
38
39 <html>
40 <head>
41     <title>Taste It Again - Display Order</title>
42 </head>
43 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"black">
44 <script type="text/javascript">
45 <!--
46 function test_it(f){
47     if(f.checkValidity()){
48         f.posted.value = "OK";
49         f.submit();
50     }
51     else{
52         alert("Please check all fields for valid data");

```

```

53         return ;
54     }
55 }
56 //-->
57 </script>
58
59 <?php
60 require "mySQL.php";
61
62 /*echo '<pre>';
63 print_r($_POST);
64 echo '</pre>';*/
65
66
67 //load ORDERS record info from database
68 $sql = "select * from ORDERS where ORDID = '$ordUID'";
69 //echo "sql: $sql<br />";
70 if (!($results = $mysqli->query($sql))){
71     die("Cannot get ORDERS record: ".$mysqli->error);
72 }
73 if ($results->num_rows != 1){
74     die("ORDERS - Wrong number of rows: ".$results->num_rows."  $sql");
75 }
76 $order = $results->fetch_assoc();
77
78 $sql = "select * from ORDERITEMS where ORDID = '$ordUID'";
79 if (!($lineitems = $mysqli->query($sql))){
80     die("ORDERITEMS - Cannot get records");
81 }
82 ?>
83
84 <table cellpadding="0" cellspacing="0" width="900" align="center" border="0">
85
86     <?php include("header.php"); ?>
87
88     <tr height="500" bgcolor="#82FA58">
89         <td colspan="2">
90             <table cellpadding="0" cellspacing="0" width="900" border="0" height="
91                 "100%">
92                 <tr valign="top">
93                     <td>
94                         <table cellpadding="0" cellspacing="0" width="900" border=
95                             "0">
96                             <tr>
97                                 <td>
98                                     <center><h1>Order Confirmation</h1></center>
99                                 </td>
100                             </tr>
101                         </table>
102                         <table cellpadding="1" cellspacing="3" style="border:1px
103                             #000000 solid" bgcolor="white" align="center">
104                             <tr>
105                                 <td colspan="2" align="center">

```

```

103         <b><ul>Delivery Address</b></ul>
104     </td>
105 </tr>
106 <tr>
107     <td>Full Name</td>
108     <td><?php echo $order['FULLNAME']; ?></td>
109 </tr>
110 <tr>
111     <td>Address</td>
112     <td><?php echo $order['DELADDLINE1']; ?></td>
113 </tr>
114 <tr>
115     <td>Address Line 2</td>
116     <td><?php echo $order['DELADDLINE2']; ?></td>
117 </tr>
118 <tr>
119     <td>City</td>
120     <td><?php echo $order['DELCITY']; ?></td>
121 </tr>
122 <tr>
123     <td>State</td>
124     <td><?php echo $order['DELSTATE']; ?></td>
125 </tr>
126 <tr>
127     <td>Zip Code</td>
128     <td><?php echo $order['DELZIP']; ?></td>
129
130 </tr>
131 <tr>
132     <td>Phone Number</td>
133     <td><?php echo $order['CONTACTPHONE']; ?></td>
134 </tr>
135 <tr>
136     <td>Time Posted</td>
137     <td><?php echo $order['TIME']; ?></td>
138 </tr>
139 </table>
140 <table align="center">
141     <tr>
142         <td>
143             <?php
144                 if ($calledBy == '')
145                     echo "<input type='button' value='Home'
146                         onclick='location.href='home.php'>";
147                 else
148                     echo "<input type='button'
149                         value='Return'
150                         onclick='window.history.back()'>";
151             ?>
152         </td>
153     </tr>
154 </table>
155 <table style="border:1px #000000 solid" align="center" bgcolor=

```



```

153         "white">
154         <tr>
155             <td><b>#</b></td><td><b>Name</b></td><td><b>Price
156             </b></td><td><b>Taxable</b></td><td><b>Qty</b></td><td><b>
157             Ext Price</b></td>
158         </tr>
159         <?php
160         $total = 0;
161         while($row = $lineitems->fetch_assoc() ){
162             echo ' <tr> ' ;
163             echo '     <td>'. $row['LINENUM']. '</td>' ;
164             echo '     <td>'. $row['NAME']. '</td>' ;
165             echo '     <td align="right">'. number_format($row['PRICE'],2).
166             '</td>' ;
167             echo '     <td align="center">'. $row['TAXABLE']. '</td>' ;
168             echo '     <td align="center">'. $row['QTY']. '</td>' ;
169             echo '     <td align="right">'. number_format($row['EXTPRICE'],2
170             ). '</td>' ;
171             echo ' </tr> ' ;
172             $total += $row['EXTPRICE'];
173         }
174         echo ' <tr><td></td><td></td><td></td><td></td><td
175         align="right"><b>Total:</b></td><td align="right">'.
176         number_format($total,2). '</td></tr>' ;
177     <?>
178     </table>
179     </td>
180 </tr>
181 </table>
182 </td>
183 <tr height="30px" bgcolor="#FFFF00">
184     <td colspan="2">
185         <?php include("footer.php"); ?>
186     </td>
187 </tr>
188 </table>
</body>
</html>

```

```

1  <?php
2  if (!@session_start()){
3      die("Cannot start session");
4  }
5
6  if (!isset($_SESSION['valid_user'])){
7      //they have not tried to login, or logged out
8      echo '<script type="text/javascript"> alert("You must login first");';
9      echo 'window.location.replace("index.php"); </script>';
10     exit();
11 }
12 ?>
13
14 <html>
15 <head>
16     <title>Taste It Again - Edit Account</title>
17 </head>
18 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"black">
19 <script type="text/javascript">
20 <!--
21 function test_it(f){
22     if((f.fName.value == '') ||
23         (f.lName.value == '') ||
24         (f.address.value == '') ||
25         (f.city.value == '') ||
26         (f.state.value == '') ||
27         (f.zipCode.value == '') ||
28         (f.email.value == '') ||
29         (f.phone.value == '')){
30         alert("All fields must be completed.");
31         return;
32     }
33
34     f.posted.value = "OK";
35     f.submit();
36 }
37 //-->
38 </script>
39
40 <?php
41 require "mysql.php";
42
43 /*echo '<pre>';
44 print_r($_POST);
45 echo '</pre>';*/
46
47 $posted    = $_POST['posted'];
48
49 if($posted == "OK"){
50     //user attempted update
51     $userid  = $_POST['userid'];
52     $fName   = $_POST['fName'];

```

```

53     $lName     = $_POST['lName'];
54     $address   = $_POST['address'];
55     $address2  = $_POST['address2'];
56     $city      = $_POST['city'];
57     $state     = $_POST['state'];
58     $zipCode   = $_POST['zipCode'];
59     $newemail  = $_POST['email'];
60     $phone     = $_POST['phone'];
61     $txtflag   = $_POST['txtflag'];
62     $mailflag  = $_POST['mailflag'];
63 }else{
64     $email = $_SESSION['email'];
65     //load account info from database
66     //get USER record
67     $sql = "select * from USERS where EMAILADD = '$email'";
68     //echo "sql: $sql<br />";
69     if (!($results = $mysqli->query($sql))){
70         die("Cannot get USER record: ".$mysqli->error);
71     }
72     if ($results->num_rows != 1){
73         die("USERS - Wrong number of rows: ".$results->num_rows."    $sql");
74     }
75     $row = $results->fetch_assoc();
76     $userid = $row['USERID'];
77     $fName  = $row['FIRSTNAME'];
78     $lName  = $row['LASTNAME'];
79     $phone  = $row['PHONE'];
80
81     //get CUSTOMER record
82     $sql = "select * from CUSTOMERS where USERID = '$userid'";
83     if (!($results = $mysqli->query($sql))){
84         die("Cannot get CUSTOMER record: ".$mysqli->error);
85     }
86     if ($results->num_rows != 1){
87         die("CUSTOMERS - Wrong number of rows: ".$results->num_rows);
88     }
89     $row = $results->fetch_assoc();
90     $address = $row['ADDLINE1'];
91     $address2 = $row['ADDLINE2'];
92     $city     = $row['CITY'];
93     $state    = $row['STATE'];
94     $zipCode  = $row['ZIP'];
95     $mailflag = $row['EMAILFLAG'];
96     $txtflag  = $row['TXTMSGFLAG'];
97 }
98
99 if ($posted == "OK"){
100     $sql1 = "UPDATE USERS SET
101         EMAILADD     = '$newemail',
102         FIRSTNAME    = '$fName',
103         LASTNAME     = '$lName',
104         PHONE        = '$phone'
105         WHERE USERID = '$userid'";

```

```

106
107 $sql2 = "UPDATE CUSTOMERS SET
108     ADDLINE1 = '$address',
109     ADDLINE2 = '$address2',
110     CITY     = '$city',
111     STATE    = '$state',
112     ZIP      = '$zipCode',
113     EMAILFLAG = '$mailflag',
114     TXTMSGFLAG = '$txtflag'
115     WHERE USERID = '$userid';";
116
117 //transaction begin with implicit autocommit off
118 if (!$mysqli->query("START TRANSACTION;")){
119     echo '<script type="text/javascript">'. "\n";
120     echo 'alert("Start transaction failed: '.$mysqli->error.'");'. "\n";
121     echo 'window.back();';
122     echo '</script>'. "\n";
123     exit();
124 }
125
126 //insert into USERS table
127 if (!$mysqli->query($sql1)){
128     //rollback
129     $err = $mysqli->error; //save error message before rollback
130     $mysqli->query("ROLLBACK;"); //must add check for rollback failure
131     echo '<script type="text/javascript">'. "\n";
132     echo 'alert("Account update failed: '.$err.'");'. "\n";
133     echo 'window.back();';
134     echo '</script>'. "\n";
135     exit();
136 }
137
138 //insert customer information
139 if (!$mysqli->query($sql2)){
140     $err = $mysqli->error; //save error message before rollback
141     //rollback
142     $mysqli->query("ROLLBACK;"); //must add check for rollback failure
143     echo '<script type="text/javascript">'. "\n";
144     echo 'alert("Account update failed: '.$err.'");'. "\n";
145     echo 'window.back();';
146     echo '</script>'. "\n";
147     exit();
148 }
149 //commit transaction
150 if ($mysqli->query("COMMIT;")){
151     $_SESSION['email'] = $newemail;
152     echo '<script type="text/javascript">'. "\n";
153     echo 'alert("Account updated");'. "\n";
154     echo 'window.location.replace("home.php");';
155     echo '</script>'. "\n";
156 }else{
157     echo '<script type="text/javascript">'. "\n";
158     echo 'alert("Commit transaction failed: '.$mysqli->error.'");'. "\n";

```

```

159     echo 'window.back();';
160     echo '</script>'. "\n";
161     exit();
162 }
163
164 }
165 ?>
166
167 <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">
168
169     <?php include("header.php"); ?>
170
171     <tr height="500" bgcolor="#82FA58">
172         <td colspan="2">
173             <table cellspacing="0" cellpadding="0" width="900" border="0" height=
174                 "100%">
175                 <tr valign="top">
176                     <td>
177 <!------- Start of main content
178 ----->
179
180                 <table cellspacing="0" cellpadding="0" width="900" border=
181                     "0">
182                     <tr>
183                         <td>
184                             <center><h1>Register</h1></center>
185                         </td>
186                     </tr>
187                 </table>
188                 <form name="update" id="update" action = '' method = "post">
189                 <table cellspacing="1" cellpadding="3" style="border:1px
190                     #000000 solid" bgcolor="#BDBDBD" align="center">
191                     <tr>
192                         <td>
193                             First Name
194                         </td>
195                         <td>
196                             <input type="text" name="fName" size="20" value=
197                                 "<?php echo $fName; ?>">
198                         </td>
199                     </tr>
200                     <tr>
201                         <td>
202                             Last Name
203                         </td>
204                         <td>
205                             <input type="text" name="lName" size="20" value=
206                                 "<?php echo $lName; ?>">
207                         </td>
208                     </tr>
209                     <tr>
210                         <td>
211                             Address

```

```

205         </td>
206         <td>
207             <input type="text" name="address" size="20"
                value="<?php echo $address; ?>">
208         </td>
209     </tr>
210     <tr>
211         <td>
212             Address Line 2
213         </td>
214         <td>
215             <input type="text" name="address2" size="20"
                value="<?php echo $address2; ?>">
216         </td>
217     </tr>
218     <tr>
219         <td>
220             City
221         </td>
222         <td>
223             <input type="text" name="city" size="20" value="
                <?php echo $city; ?>">
224         </td>
225     </tr>
226     <tr>
227         <td>
228             State
229             <input type="text" name="state" size="3" value="
                <?php echo $state; ?>">
230         </td>
231         <td>
232             Zip Code
233             <input type="text" name="zipCode" size="5" value
                ="<?php echo $zipCode; ?>">
234         </td>
235     </tr>
236     <tr>
237         <td>
238             Phone Number
239         </td>
240         <td>
241             <input type="text" name="phone" size="20" value=
                "<?php echo $phone; ?>">
242         </td>
243     </tr>
244     <tr>
245         <td>
246             Email Address
247         </td>
248         <td>
249             <input type="text" name="email" size="30" value=
                "<?php echo $email; ?>">
250         </td>

```

```

251         </tr>
252     <tr>
253         <td>
254             Send me email coupons
255         </td>
256         <td>
257             <input type="radio" name="mailflag" value="1"
258             <?php echo ($mailflag == "1")?"checked":""; ?> >Y
259             <input type="radio" name="mailflag" value="0"
260             <?php echo ($mailflag == "0")?"checked":""; ?> >N
261         </td>
262     </tr>
263     <tr>
264         <td>
265             Send me txt message coupons
266         </td>
267         <td>
268             <input type="radio" name="txtflag" value="1"
269             <?php echo ($txtflag == "1")?"checked":""; ?> >Y
270             <input type="radio" name="txtflag" value="0"
271             <?php echo ($txtflag == "0")?"checked":""; ?> >N
272         </td>
273     </tr>
274 </table>
275 <table align="center">
276     <tr>
277         <td>
278             <input name="btnSave" type="button" value="Save
279             Changes" onclick="test_it(this.form);"/>
280             <!--<input type="reset" value="Reset">-->
281         </td>
282     </tr>
283 </table>
284 <input name="posted" type="hidden" value="">
285 <input name="userid" type="hidden" value=<?php echo $userid;
286 ?>>
287 </form>
288 </td>
289 </tr>
290 </table>
291 </td>
292 </tr>
293 </table>
294 </body>
295 </html>
296
297

```

```
1  <table cellspacing="0" cellpadding="0" width="900" border="0">
2      <tr>
3          <td>
4              <center><font color="#04B404"><B>Copyright Info</B></font></center>
5          </td>
6      </tr>
7  </table>
```



```

1
2 <style type="text/css">
3 .nav a:link {color:#04B404; text-decoration:none; font-family: arial black;
font-weight: bold}
4 .nav a:visited {color:#04B404; font-family: arial black; font-weight: bold}
5 .nav a:hover {text-decoration:none; color:#000000; font-family: arial black;
font-weight: bold}
6 .nav a:active {font-family: arial black; font-weight: bold}
7
8 .header a:link {color:#04B404; text-decoration:none;}
9 .header a:visited {color:#04B404;}
10 .header a:hover {text-decoration:underline;}
11 .header a:active {}
12
13 .vieworder a:link {color:#FFFF00; text-decoration:; font-weight: bold;}
14 .vieworder a:visited {color:#FFFF00;}
15 .vieworder a:hover {text-decoration:; color:#000000}
16 .vieworder a:active {}
17
18 .button_link a:link {text-decoration:none;}
19 .button_link a:visited {}
20 .button_link a:hover {text-decoration:none;}
21 .button_link a:active {}
22
23 .welcome {
24     color: #FFFF00;
25     font-family: verdana;
26     font-size: 12px;
27 }
28 </style>
29
30 <?php
31 $firstname = $_SESSION['firstname'];
32 $firstname = ($firstname == '')?"Guest":$firstname;
33 $isAdmin = $_SESSION['isAdmin'];
34 $isOwner = $_SESSION['isOwner'];
35 $isCustomer = $_SESSION['isCustomer'];
36 $email = $_SESSION['email'];
37
38 //unset($_SESSION['userCatList']);
39 //get category list for users (Admin users have a real-time category list when
administering categories and products)
40 if (!isset($_SESSION['userCatList'])) {
41     if ($result = @$mysqli->query("select CATID, NAME from CATEGORIES")) {
42         $userCatList = array();
43         while ($row = $result->fetch_assoc()) {
44             $userCatList[intval($row['CATID'])] = $row['NAME'];
45         }
46         $_SESSION['userCatList'] = $userCatList;
47     } else {
48         echo '<script type="text/javascript"> alert("Error - cannot get category list: '
.$mysqli->error.'");</script>';
49     }

```

```

50 }else{
51     $userCatList = $_SESSION['userCatList'];
52     /*
53     echo "<pre>";
54     print_r($userCatList);
55     echo "</pre>";*/
56 }
57
58 ?>
59 <link rel="stylesheet" href="styles.css" type="text/css">
60 <tr height="100px" bgcolor="#04B404">
61     <td>
62         <table cellpadding="0" cellspacing="0" align="center" border="0">
63             <tr align="center">
64                 <td align="center">
65                     <center><font color="#FFFF00" face="arial black"><h1>T a s
66                         t e &nbsp;   I t &nbsp;   A g a i n</h1></font></center>
67                 </td>
68             </tr>
69             <tr>
70                 <td>
71                     <center><font face="fantasy" color="#FFFF00">- F i n e
72                         &nbsp;   J a m a i c a n &nbsp;   D i n i n g -
73                     </font></center><br />
74                     <!--
75                         271 Glenwood Avenue Bloomfield, NJ 07003<br />
76                     Phone: (973)743-5140
77                     -->
78                 </td>
79             </tr>
80         </table>
81     </td>
82     <tr width="100%" height="30px" bgcolor="#FFFF00">
83         <td colspan="2">
84             <table cellpadding="0" cellspacing="0" width="900" border="0" bgcolor=
85                 "#FFFF00">
86                 <tr>
87                     <div id='cssmenu'>
88                         <ul>
89                             <li class='active '><a href='home.php'><span>HOME
90                                 </span></a></li>
91                             <li class='has-sub '><a href='menu.php?cat=000000'
92                                 ><span>MENU</span></a>
93                                 <ul>
94                                     <li><a href="menu.php?cat=000000">All Menu
95                                         Items </a></li>
96                                     <?php
97                                     foreach ($userCatList as $key => $value){
98                                         if ($value != "Merchandise"){ //merchandise
99                                             has its own menu
100                                         echo '<li><a href="menu.php?cat='.$key.
101                                             '>'.$value.'</a></li>'."\\n";
102                                     }

```

```

94         }
95     ?>
96     </ul>
97 </li>
98 <li><a href='merch.php'><span>MERCHANDISE</span></a></li>
99 <li><a href='info.php'><span>INFORMATION</span></a></li>
100 </ul>
101 </div>
102 </tr>
103 </table>
104 </td>
105 </tr>
106 <tr width="100%" height="25px" bgcolor="#40FF00">
107 <td colspan="2">
108 <table cellpadding="0" cellspacing="0" width="900" border="0" bgcolor=
"#04B404">
109 <tr>
110 <td>
111 <span class="welcome">
112 &nbsp; Welcome, <?php echo $firstname; ?>!
113 <?php
114 if (count($_SESSION['cart']) > 0){
115     echo '<span class="welcome"> | </span><span
class="vieworder"><a href="viewcart.php">View
Order</a></span>';
116 }
117 ?>
118 </span>
119
120 <!--
121 <?php
122 if($isCustomer == 'Y'){
123     echo 'CUSTOMER = YES';
124 }else{
125     echo 'CUSTOMER = NO';
126 }
127 ?>
128 -->
129
130 </td>
131 <form name="login" id="login" action="homelogin.php" method=
"POST">
132 <td align="right">
133 <span class="welcome">
134 Email <input type="text" name="email" size="20">
135 Password <input type="password" name="password" size=
"20">
136 </span>
137 <?php
138 if (!$isCustomer == 'Y'){
139     echo '<input type="submit" value="Login">';
140 }else{
141     echo '<span class="button_link"><a

```

```

                                href="homelogout.php"><input type="button"
                                value="Logout"></a></span>' ;
142                                }
143                                ?>
144                                <?php
145                                if ($isCustomer == 'Y'){
146                                echo '<span class="button_link"><a
                                href="editAccount.php"><input type="button"
                                value="Edit Account"></a></span>' ;
147                                }else{
148                                echo '<span class="button_link"><a
                                href="register.php"><input type="button"
                                value="Register"></a></span>' ;
149                                }
150                                ?>
151                                </td>
152                                </form>
153                                </tr>
154                                </table>
155                                </td>
156                                </tr>
157                                <?php
158                                if (($isAdmin == 'Y')){
159                                echo '<tr width="100%" height="25px" bgcolor="#40FF00">' ;
160                                echo '    <td colspan="2">' ;
161                                echo '        <table cellpadding="0" cellspacing="0" width="900" border="0"
                                bgcolor="#04B404">' ;
162                                echo '            <tr>' ;
163                                echo '                <td align="left">' ;
164                                echo '                    <span class="welcome">' ;
165                                echo '                        &nbsp; <b>- Admin Menu -</b> &nbsp; <span
                                class="button_link"><a href="categoryAdmin.php"><input type="button"
                                value="Categories"></a><a href="productAdmin.php"><input type="button"
                                value="Products"></a></span>' ;
166                                echo '                    </span>' ;
167                                echo '                </td>' ;
168                                echo '            </tr>' ;
169                                echo '        </table>' ;
170                                echo '    </td>' ;
171                                echo '</tr>' ;
172                                }
173                                ?>
174
175                                <?php
176                                if (($isOwner == 'Y')){
177                                echo '<tr width="100%" height="25px" bgcolor="#40FF00">' ;
178                                echo '    <td colspan="2">' ;
179                                echo '        <table cellpadding="0" cellspacing="0" width="900" border="0"
                                bgcolor="#04B404">' ;
180                                echo '            <tr>' ;
181                                echo '                <td align="left">' ;
182                                echo '                    <span class="welcome">' ;
183                                echo '                        &nbsp; <b>- Owner Menu -</b> &nbsp; <span

```

```
class="button_link"><a href="vieworders.php"><input type="button"
value="View Orders"></a></span>' ;
184     echo '                </span>' ;
185     echo '            </td>' ;
186     echo '        </tr>' ;
187     echo '    </table>' ;
188     echo ' </td>' ;
189     echo '</tr>' ;
190 }
191 ?>
```

[illegible]

```
49         <td>
50             
52         </td>
53         <td>
54             
56         </td>
57     </tr>
58 </table>
59 <tr height="30px" bgcolor="#FFFF00">
60     <td colspan="2">
61         <?php include("footer.php"); ?>
62     </td>
63 </tr>
64 </table>
65 </body>
66 </html>
```

```
1  <?php
2  include "mysql.php";
3
4  if (!@session_start()){
5      die("Cannot start session");
6  }
7
8  if (!isset($_SESSION['valid_user'])){
9      //they have not tried to login, or logged out
10     echo '<script type="text/javascript"> alert("You must login first");';
11     echo 'window.location.replace("index.php"); </script>';
12     exit();
13 }
14
15 $email = strtolower($_POST['email']);
16 $password = $_POST['password'];
17 $hash = md5($password);
18
19 if (!$results = $mysqli->query("SELECT * from USERS where EMAILADD = '$email' AND
PWHASH = '$hash'")){
20     die("Query failed");
21 }
22 if ($results->num_rows > 1){
23     die("Query error - too many rows returned.");
24 }
25
26 $row = $results->fetch_assoc();
27 if (!$row){
28     echo '<script type="text/javascript"> alert("Invalid username/password");';
29     echo 'window.location = "'.$_SERVER['HTTP_REFERER'].'"';
30     echo '</script>';
31     exit();
32 }
33
34 $_SESSION['firstname'] = $row['FIRSTNAME'];
35 $_SESSION['isAdmin'] = $row['ADMINFLAG'];
36 $_SESSION['isOwner'] = $row['OWNERFLAG'];
37 $_SESSION['isCustomer'] = $row['CUSTFLAG'];
38 $_SESSION['email'] = $email;
39
40 /*
41 //debug messages
42 echo "firstname  ".$_SESSION['firstname']." <br/>";
43 echo "isAdmin    ".$_SESSION['isAdmin']." <br/>";
44 echo "isOwner     ".$_SESSION['isOwner']." <br/>";
45 echo "isCustomer  ".$_SESSION['isCustomer']." <br/>";
46 echo "email       ".$_SESSION['email']." <br/>";
47 */
48
49 echo '<script type="text/javascript">';
50 echo 'alert("Login Successful");';
51 echo 'window.location = "'.$_SERVER['HTTP_REFERER'].'"';
52 echo '</script>';
```


53 

```
1  <?php
2  include "mysql.php";
3
4  if (!@session_start()){
5      die("Cannot start session");
6  }
7
8  if (!isset($_SESSION['valid_user'])){
9      //they have not tried to login, or logged out
10     echo '<script type="text/javascript"> alert("You must login first");';
11     echo 'window.location.replace("index.php"); </script>';
12     exit();
13 }
14 //echo '<pre>';
15 //print_r($_SESSION);
16 //echo '</pre>';
17
18 unset($_SESSION['email']);
19 unset($_SESSION['firstname']);
20 unset($_SESSION['isAdmin']);
21 unset($_SESSION['isOwner']);
22 unset($_SESSION['isCustomer']);
23
24 echo '<script type="text/javascript">';
25 echo 'alert("You have been logged out.");';
26 echo 'window.location = "."'home.php'";
27 echo '</script>';
28
29 ?>
```

```

1  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "
    http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
2  <html xmlns="http://www.w3.org/1999/xhtml">
3
4  <head>
5  <meta content="text/html; charset=utf-8" http-equiv="Content-Type" />
6  <title>Create Account</title>
7  <style type="text/css">
8  .auto-style1 {
9      text-align: right;
10 }
11 </style>
12 </head>
13
14 <body>
15
16 <script type="text/javascript">
17 <!--
18 function test_it(f){
19     if((f.fName.value == '') ||
20         (f.lName.value == '') ||
21         (f.email.value == '') ||
22         (f.password.value == '') ||
23         (f.password2.value == '') ||
24         (f.phone.value == '')){
25         alert("All fields must be completed.");
26         return;
27     }
28
29     if(f.password.value != f.password2.value){
30         alert("Passwords do not match.");
31         return;
32     }
33     f.posted.value = "OK";
34     f.submit();
35 }
36 //-->
37 </script>
38
39 <?php
40 require "mysql.php";
41 $fName     = $_POST['fName'];
42 $lName     = $_POST['lName'];
43 $email     = $_POST['email'];
44 $password  = $_POST['password'];
45 $phone     = $_POST['phone'];
46 $posted    = $_POST['posted'];
47 $hash      = md5($password);
48
49 echo "<br>posted: $posted";
50
51 if ($posted == "OK"){
52     $sql = "insert into USERS (EMAILADD, PWHASH, FIRSTNAME, LASTNAME, PHONE) VALUES('

```

```

53     $email', '$hash', '$fName', '$lName', '$phone');"
54     echo "<br>sql: $sql";
55
56     if($result = $mysqli->query($sql)){
57         echo '<script type="text/javascript"> alert("Account created"); </script>';
58     }else{
59         //echo '<script type="text/javascript"> alert("Account creation failed:
60         "+$mysqli->error); </script>';
61         echo '<script type="text/javascript"> alert($mysqli->error); </script>';
62     }
63 }
64 ?>
65
66 <h1>Create Account</h1>
67 <table>
68 <form action="" method="post">
69     <tr><td class="auto-style1">First Name:         </td><td> <input name="fName"
70     type="text"      value="<?php echo $fName; ?>" /></td></tr>
71     <tr><td class="auto-style1">Last Name:         </td><td> <input name="lName"
72     type="text"      value="<?php echo $lName; ?>" /></td></tr>
73     <tr><td class="auto-style1">E-Mail Address:     </td><td> <input name="email"
74     type="text"      value="<?php echo $email ?>" /></td></tr>
75     <tr><td class="auto-style1">Password:         </td><td> <input name="password"
76     type="password" value="" /></td></tr>
77     <tr><td class="auto-style1">Re-enter Password: </td><td> <input name="password2"
78     type="password" value="" /></td></tr>
79     <tr><td class="auto-style1">Phone:             </td><td> <input name="phone"
80     type="text"      value="<?php echo $phone; ?>" /></td></tr>
81     <tr><td><input name="btnRegister" type="button" value="Register" onclick=
82     "test_it(this.form);" /></td></tr>
83     <input name="posted" type="hidden" value="">
84 </form>
85 </table>
86
87 </body>
88
89 </html>

```

```

1  <html>
2  <head>
3      <title>Project Login</title>
4  </head>
5  <script type="text/javascript" >
6  function test_it(f)
7  {
8      //alert("Test");
9      if (f.u_id.value == "" || f.u_pwd.value == "")
10     {
11         alert("You have to enter a user ID and password!");
12         return;
13     }
14
15     //changes to catch XSS and SQL injection
16     if ((f.u_id.value.indexOf("<") != -1) || (f.u_pwd.value.indexOf("<") != -1) ||
17     (f.u_id.value.indexOf("'") != -1) || (f.u_pwd.value.indexOf("'") != -1))
18     {
19         alert("You have illegal characters in user ID or password!");
20         return;
21     }
22
23     //alert(f.u_id.value + ' ' + f.u_pwd.value ) ;
24     f.submit();
25
26 }
27
28 </script>
29
30 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"white">
31     <table cellpadding="0" cellspacing="0" border="0" width="500" align="center">
32         <tr>
33             <td width="300">
34                 <br /><br /><br /><br />
35                 <form action = "cPanelLogin.php" method = "POST" name="login" id="login">
36                 <table cellpadding="3" cellspacing="1" style="border:1px solid
bgcolor="#BDBDBD" align="center">
37                     <tr>
38                         <td width="300" colspan="2">
39                             <center><h1>Project Login</h1></center>
40                         </td>
41                     </tr>
42
43                     <tr>
44                         <td width="75">
45                             Login:
46                         </td>
47                         <td width="225">
48                             <input type="text" name="u_id" size="30">
49                         </td>
50                     </tr>
51

```

```
52         <tr>
53             <td width="75">
54                 Password:
55             </td>
56             <td width="225">
57                 <input type="password" name="u_pwd" size="30">
58             </td>
59         </tr>
60
61     </table>
62     <table align="center">
63         <tr>
64             <td>
65                 <input type = "button" value = "Login" onclick=
66                     "test_it(this.form);">
67                 <input type="reset" value="Reset">
68             </td>
69         </tr>
70     </table>
71     </form><br>
72     <table cellpadding="0" cellspacing="0" align="center">
73         <tr>
74             <td>
75                 Kevin Miller & Matt Haight<br>
76                 Final Project<br>
77                 CMPT-483 Database Systems<br>
78                 Professor Katherine G. Herbert, Ph.D.<br>
79                 Montclair State University<br>
80                 Fall 2012
81             </td>
82         </tr>
83     </table>
84
85 </td>
86 </tr>
87 </table>
88 </body>
89 </html>
90
```

```

1  <?php
2  //connect to database
3  require "mysql.php";
4
5  if (!@session_start()){
6      die("Cannot start session");
7  }
8
9  if (!isset($_SESSION['valid_user'])){
10     echo '<script type="text/javascript"> alert("You must login.");';
11     echo 'window.location.replace("index.php"); </script>';
12     exit();
13 }
14 ?>
15 <html>
16 <head>
17     <title>Taste It Again - Information</title>
18     <?php //include("head.php"); ?>
19 </head>
20
21 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"black">
22
23     <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">
24
25         <?php include("header.php"); ?>
26
27         <tr height="500" bgcolor="#82FA58">
28             <td colspan="2">
29                 <table cellspacing="0" cellpadding="0" width="900" border="0" height=
"100%">
30                     <tr valign="top">
31                         <td>
32 <!-- Start of added content
----->
33
34                         <center><h1>Information Coming Soon!</h1><center>
35
36                         </td>
37                     </tr>
38                 </table>
39             </td>
40         </tr>
41         <tr height="30px" bgcolor="#FFFF00">
42             <td colspan="2">
43                 <?php include("footer.php"); ?>
44             </td>
45         </tr>
46     </table>
47 </body>
48 </html>
49

```

```
1  <?php
2  //connect to database
3  require "mySQL.php";
4
5  if (!@session_start()){
6      die("Cannot start session");
7  }
8
9  if (!isset($_SESSION['valid_user'])){
10     echo '<script type="text/javascript"> alert("You must login.");';
11     echo 'window.location.replace("index.php"); </script>';
12     exit();
13 }
14 //category filter from main menu
15 // $cat = $_GET['cat']; //bugfix 2012-12-16 KSM
16 if(isset($_GET['cat']))
17     $cat = $_GET['cat'];
18 else
19     $cat = $_POST['cat'];
20
21
22
23 $sql = "select * from PRODUCTS".((intval($cat) > 0) ? " where CATID = '$cat' " : "").
order by CATID";
24 //echo $sql."<br />";
25 if (!($menuResults = $mysqli->query($sql))){
26     die("Error - cannot get menu.\n$sql");
27 }
28
29 //get current list of all categories - created in header.php
30 $userCatList = $_SESSION['userCatList'];
31
32 //get, or create cart
33 //unset($_SESSION['cart']); //for debugging
34 if (isset($_SESSION['cart'])){
35     $cart = $_SESSION['cart'];
36 }else{
37     //echo "new cart!<br />";
38     $cart = array();
39 }
40
41 /*
42 //debug messages
43 echo "<pre>";
44 echo "session cart: <br />";
45 print_r($cart);
46 echo "</pre>";
47 */
48
49 /*
50 //debug messages
51 echo "<pre>";
52 echo "POST: <br />";
```



```
53  print_r($_POST);
54  echo "</pre>";
55  */
56
57  /*
58  //debug messages
59  echo "<pre>";
60  echo "GET: <br/>";
61  print_r($_GET);
62  echo "</pre>";
63  */
64
65  //update cart
66  foreach($_POST as $key => $value){
67      $arr = explode("-", $key);
68      if($arr[0] == "key"){
69          //if qty = 0, delete from cart; otherwise add/update
70          if($value == 0){
71              unset($cart[$arr[1]]);
72          }
73          else{
74              $cart[$arr[1]] = $value;
75          }
76      }
77  }
78  //put updated cart back into session
79  $_SESSION['cart'] = $cart;
80
81  /*
82  //debug messages
83  echo "<pre>";
84  echo "SESSION: <br />";
85  print_r($_SESSION);
86  echo "</pre>";
87  */
88
89  /*
90  //debug messages
91  echo "<pre>";
92  echo "updated cart: <br />";
93  print_r($cart);
94  echo "</pre>";
95  */
96
97  if(isset($cart)){
98      if(count($cart)==0)
99          $cartStatusMsg = "You have 0 items in cart";
100     else{
101         $itemCount = 0;
102         foreach($cart as $key => $value)
103             $itemCount += $value;
104
105         $cartStatusMsg = "You have $itemCount items in your cart.";
```

```

106     }
107 }
108 ?>
109
110 <script type="text/javascript" >
111 function validate(f){
112     if(f.checkValidity()){
113         f.submit();
114     }else{
115         alert("Invalid data - Please check all fields");
116         return;
117     }
118 }
119 </script>
120
121 <script type="text/javascript" >
122 //function viewCart(f){
123 //    alert("viewing cart");
124 //    f.action="viewcart.php";
125 //    alert (f.action);
126 //    f.submit();
127 //}
128 </script>
129
130 <html>
131 <head>
132     <?php
133         if (isset($_POST['btnViewCart'])){
134             //if "View Cart" button was pressed and cart is not empty, redirect to
135             //viewcart.php after updating cart
136             echo ' <meta HTTP-EQUIV="REFRESH" content="0; url=viewcart.php">'. "\n";
137         }
138     ?>
139     <title>Taste It Again - Menu</title>
140 </head>
141 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
142 "black">
143
144     <table cellpadding="0" cellspacing="0" width="900" align="center" border="0">
145
146         <tr height="500" bgcolor="#82FA58">
147             <td colspan="2">
148                 <table cellpadding="0" cellspacing="0" width="900" border="0" height=
149                 "100%">
150                     <tr valign="top">
151                         <td>
152                             <!-- CONTENT -->
153                             <form name="menu" action="<?php echo $_SERVER['SCRIPT_NAME']
154                             ";?>" id="menu" method = "POST">
155                             <table cellpadding="0" cellspacing="0" width="900" border=
156                             "0">

```

```

154         <?php
155             if($cartStatusMsg != ""){
156                 echo "<tr><td>$cartStatusMsg</td></tr>\n";
157             }
158         ?>
159         <tr>
160             <td>
161                 <center><h1>Menu</h1></center>
162             </td>
163         </tr>
164     <?php
165         $currentCatID = 0;
166         $bgColor = 'white';
167         if($product = $menuResults->fetch_assoc()){ //there
            is at least one record
168             while (true){ //break when no more records
169                 $currentCatID = intval($product['CATID']);
170                 $currentCatName = $userCatList[$currentCatID
                    ];
171
172                 //output new category header
173                 echo "<tr>\".\n";
174                 echo "    <td>\".\n";
175                 echo "        <h2>$currentCatName</h2>\n";
176                 echo "    </td>\".\n";
177                 echo "</tr>\".\n";
178
179                 //alternate background colors
180                 if ($bgColor != '#BDBDBD'){
181                     $bgColor = '#BDBDBD';
182                 }else{
183                     $bgColor = 'white';
184                 }
185
186                 //print category header
187                 echo '<tr>\".\n';
188                 echo '    <td>\".\n';
189                 echo '        <table cellspacing="1"
                    cellpadding="1" style="border:1px #000000
                    solid" bgcolor="\".$bgColor.\""
                    align="center" width="800">\".\n';
190                 echo '            <tr>\".\n';
191                 echo '                <td width="150">\".\n';
192                 echo '
                    <b><h3>Product</h3></b>\".\n';
193                 echo '                </td>\".\n';
194                 echo '                <td width="75">\".\n';
195                 echo '
                    <center><b><h3>Price</h3></b></center>\".\n';
196                 echo '                </td>\".\n';
197                 echo '                <td width="150">\".\n';
198                 echo '
                    <center><b><h3>Quantity</h3></b></center>\".

```

```

199         "\n";
200     echo '                </td>' . "\n";
201     echo '            </tr>' . "\n";
202
203     while (true){ //break when caetgory changes
204         //print record
205         echo '<tr>' . "\n";
206         echo '    <td>' . "\n";
207         echo '<span title="' . $product[
208             'DESCRIPTION' ]. '">' . "\n";
209         echo '<b>' . $product['NAME' ]. '</b>' . "\n";
210         echo '    </td>' . "\n";
211         echo '    <td>' . "\n";
212         echo '        <center>$' . number_format(
213             $product['PRICE' ], 2) . '</center>' . "\n";
214         echo '    </td>' . "\n";
215         echo '    <td>' . "\n";
216         $pKey = 'key-' . $product['PRODID' ];
217         $pQty = intval($cart[$product['PRODID'
218             ]]);
219         echo '        <center>
220             <input type="text"
221             name="' . $pKey . '"
222             size="2"
223             value="' . $pQty . '">
224             </center>' . "\n";
225         echo '    </td>' . "\n";
226         echo '</tr>' . "\n";
227
228         //get next record
229         if (!($product = $menuResults->
230             fetch_assoc())){
231             //no more records
232             break;
233         }
234
235         //check if caategory changes
236         if (intval($product["CATID"]) !=
237             $currentCatID){
238             break;
239         } //end if
240     } //end while same category
241
242     //print end of category table
243     echo '    </table>' . "\n";
244     echo ' </td>' . "\n";
245     echo ' </tr>' . "\n";
246
247     if (!($product)){
248         //no more records
249         break;
250     }

```

```

245         } //end while records exist
246     } //end if get record
247     ?>
248     </table>
249     <table align="center">
250         <tr>
251             <td>
252                 <?php
253                 if((count($cart) == 0)){ //cart is empty
254                     echo '<input type="submit"
                        name="btnCreateOrder" value="Create Order">'
                        . "\n";
255                 } else {
256                     echo '<input type="submit"
                        name="btnUpdateOrder" value="Update Order">'
                        . "\n";
257                     echo '<input type="submit"
                        name="btnViewCart" value="View Cart" >' . "\n";
258                 }
259                 ?>
260                 <input type="hidden" name="cat" value="<?php
                    echo $cat; ?>">
261             </td>
262         </tr>
263     </table>
264 </form>
265 </td>
266 </tr>
267 </table>
268 </td>
269 </tr>
270 <tr bgcolor="#82FA58">
271     <td colspan="2">
272         &nbsp;
273     </td>
274 </tr>
275 <tr height="30px" bgcolor="#FFFF00">
276     <td colspan="2">
277         <?php include("footer.php"); ?>
278     </td>
279 </tr>
280 </table>
281 </body>
282 </html>
283
284
285

```

```

1  <?php
2  //connect to database
3  require "mysql.php";
4
5  if (!@session_start()){
6      die("Cannot start session");
7  }
8
9  if (!isset($_SESSION['valid_user'])){
10     echo '<script type="text/javascript"> alert("You must login.");';
11     echo 'window.location.replace("index.php"); </script>';
12     exit();
13 }
14 ?>
15 <html>
16 <head>
17     <title>Taste It Again - Merchandise</title>
18     <?php //include("head.php"); ?>
19 </head>
20
21 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"black">
22
23     <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">
24
25         <?php include("header.php"); ?>
26
27         <tr height="500" bgcolor="#82FA58">
28             <td colspan="2">
29                 <table cellspacing="0" cellpadding="0" width="900" border="0" height=
"100%">
30                     <tr valign="top">
31                         <td>
32 <!-- CONTENT -->
33                             <center><h1>Merchandise</h1><center>
34                             </td>
35                         </tr>
36                         <tr>
37                             <td align="center" valign="center">
38                                 <h1>Coming Soon!</h1>
39                             </td>
40                         </tr>
41                     </table>
42                 </td>
43             </tr>
44             <tr height="30px" bgcolor="#FFFF00">
45                 <td colspan="2">
46
47                     <?php include("footer.php"); ?>
48
49                 </td>
50             </tr>
51 </table>

```

```
52     </body>
53     </html>
54
```

```
1  <?php
2  //connect to database and table
3  $db_host = 'localhost';
4  $db_user = 'cmpt483a_root';
5  $db_pwd = '&6Kmz[FOfuH$';
6  $database = 'cmpt483a_tasteitagain';
7  $mysqli = new mysqli($db_host, $db_user, $db_pwd, $database);
8  if ($mysqli->connect_error) {
9      die('Connect Error (' . $mysqli->connect_errno . ') '
10         . $mysqli->connect_error);
11  }
12
13  ?>
```



```
1  <?php
2  //connect to database
3  require "mysql.php";
4
5  if (!@session_start()){
6      die("Cannot start session");
7  }
8
9  if (!isset($_SESSION['valid_user'])){
10     echo '<script type="text/javascript">'. "\n";
11     echo 'alert("You must login.");'. "\n";
12     echo 'window.location.replace("index.php");'. "\n";
13     echo '</script>'. "\n";
14     exit();
15 }
16 /*
17 echo "firstname   " . $_SESSION['firstname'] . "    <br/>";
18 echo "isAdmin     " . $_SESSION['isAdmin'] . "    <br/>";
19 echo "isOwner      " . $_SESSION['isOwner'] . "    <br/>";
20 echo "isCustomer   " . $_SESSION['isCustomer'] . "  <br/>";
21 echo "email        " . $_SESSION['email'] . "      <br/>";
22 */
23
24 if($_SESSION['isAdmin'] != 'Y'){
25     echo '<script type="text/javascript">'. "\n";
26     echo 'alert("Only administrators can use this page");'. "\n";
27     echo 'window.history.back();'. "\n";
28     echo '</script>'. "\n";
29     exit();
30 }
31
32 ?>
33
34 <script type="text/javascript" >
35 function validate(f){
36     if(f.checkValidity()){
37         f.submit();
38     }else{
39         alert("Invalid data - Please check all fields");
40         return;
41     }
42 }
43 </script>
44
45 <html>
46 <head>
47     <title>Taste it again - Product Admin</title>
48 </head>
49 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"black">
50     <table cellpadding="0" cellspacing="0" width="900" align="center" border="0">
51
52         <?php include("header.php"); ?>
```

```

53
54         <tr height="500" bgcolor="#82FA58">
55             <td colspan="2">
56                 <table cellpadding="0" cellspacing="0" width="900" border="0" height=
                    "100%">
57                     <tr valign="top">
58                         <td><center>
59 <!-- Start
-----
----->
60 <?php
61
62 /*
63 echo "<pre>\n";
64 print_r($_POST);
65 echo "</pre>\n";
66 */
67
68 //operation variables are the operation being performed by admin
69 $operation = $_POST['operation']; //SQL Operation UPDATE, INSERT, or DELETE
70 if ($_POST['updateFlag'] == "UPDATE")
71     $operation = "UPDATE";
72
73 //user-input fields for new record
74 $pProdID = $_POST['pProdID'];
75 $pCatID = $_POST['pCatID'];
76 $pCatName = $_POST['pCatName'];
77 $pName = $_POST['pName'];
78 $pDesc = $_POST['pDesc'];
79 $pPrice = $_POST['pPrice'];
80 $pTax = (strtoupper($_POST['pTax']) == "Y") ? "1" : "0";
81 // $pCstart = !(strtotime($_POST['pCstart'])) ? "NULL" : $_POST['pCstart'];
82 // $pCend = !(strtotime($_POST['pCend'])) ? "NULL" : $_POST['pCend'];
83 $pHide = (strtoupper($_POST['pHide']) == "Y") ? "1" : "0";
84
85 //filter products table
86 $filterCatID = $_POST['filterCatID'];
87
88 //default values when user selected Edit
89 $edProdID = $_POST['edProdID'];
90 $edName = $_POST['edName'];
91 $edDesc = $_POST['edDesc'];
92 $edCatID = $_POST['edCatID'];
93 $edCatName = $_POST['edCatName'];
94 $edPrice = $_POST['edPrice'];
95 $edTax = ($_POST['edTax'] == "1") ? "Y" : "N";
96 // $edCstart = (($_POST['edCstart'] == '0000-00-00') ? "" : $_POST['edCstart']);
97 // $edCend = (($_POST['edCend'] == '0000-00-00') ? "" : $_POST['edCend']);
98 $edHide = ($_POST['edHide'] == "1") ? "Y" : "N";
99
100 //buttons from each row
101 $btnEditProduct = $_POST['btnEditProduct'];
102 $btnDeleteProduct = $_POST['btnDeleteProduct'];

```

```

103     if($btnDeleteProduct == "Delete")
104         $operation = "DELETE";
105
106     $posted      = $_POST['posted'];           //user submitted a form
107     $table       = "PRODUCTS";
108
109     //echo"operation      $operation      <br />\n";
110     //echo"keyFieldData $keyFieldData<br />\n";
111     //echo"keyFieldName $keyFieldName<br />\n";
112     //echo"fieldData    $fieldData    <br />\n";
113     //echo"fieldName    $fieldName    <br />\n";
114     //echo"table        $table        <br />\n";
115
116     //get list of categories
117     if (!(($catList = $mysqli->query("select CATID, NAME from CATEGORIES;"))){
118         die("Cannot get category list");
119     }
120
121     /*echo "posted: $posted<br />";
122     echo "operation: $operation<br />";
123     echo "keyFieldName: $keyFieldName<br />";
124     echo "keyFieldData: $keyFieldData<br />";
125     */
126
127     //perform user selected operation
128     if ($posted == "Y"){
129         if (($operation == "UPDATE") && ($pProdID != ""))
130         {
131             /*$sql="UPDATE {$table} SET NAME                = '{$pName}',
132                                     DESCRIPTION            = '{$pDesc}',
133                                     CATID                  = '{$pCatID}',
134                                     PRICE                   = '{$pPrice}',
135                                     TAXABLE                 = '{$pTax}',
136                                     COUPONSTARTDATE         = '{$pCstart}',
137                                     COUPONENDDATE           = '{$pCend}',
138                                     HIDEFLAG                = '{$pHide}'
139                                     WHERE PRODID = '{$pProdID}';";*/
140
141             $sql="UPDATE {$table} SET NAME                = '{$pName}',
142                                     DESCRIPTION            = '{$pDesc}',
143                                     CATID                  = '{$pCatID}',
144                                     PRICE                   = '{$pPrice}',
145                                     TAXABLE                 = '{$pTax}',
146                                     HIDEFLAG                = '{$pHide}'
147                                     WHERE PRODID = '{$pProdID}';";
148         }else{
149             if (($operation == "DELETE") && ($edProdID != ""))
150             {
151                 $sql="DELETE FROM {$table} WHERE PRODID = '{$edProdID}';";
152                 //delete $ed*
153                 unset($edProdID, $edName, $edDesc, $edCatID, $edCatName, $edPrice, $edTax,
154                     $edCstart, $edCend, $edHide);
155             }else{

```

```

155         if ($operation == "INSERT")
156         {
157             //          $sql="INSERT INTO {$table} (NAME, DESCRIPTION, CATID, PRICE, TAXABLE,
COUPONSTARTDATE, COUPONENDDATE, HIDEFLAG)
158             //          VALUES ('$pName', '$pDesc', '$pCatID', '$pPrice',
'$pTax', '$pCstart', '$pCend', '$pHide');" ;
159
160             $sql="INSERT INTO {$table} (NAME      , DESCRIPTION, CATID      , PRICE
, TAXABLE, HIDEFLAG)
161             VALUES ('$pName', '$pDesc'      , '$pCatID', '$pPrice
, '$pTax', '$pHide');" ;
162
163         }else{
164             if($btnEditProduct == "Edit"){ //user selected edit - no operation
165                 //if user is editing existing product, get it's CATID
166                 $pCatID = $edCatID;
167             }else
168                 echo "Error - Operation or values are incorrect. <br />";
169         }
170     }
171 }
172
173 if ($sql != "")
174 {
175     //echo "<br>attempting to run query $sql" . "<br>";
176     if (!(($results = $mysqli->query($sql))){
177         echo("Operation query failed.<br />");
178         echo("sql: $sql<br />");
179     }
180 }
181
182
183 //disply edit/input table
184 echo "<h1>Edit Table: {$table}</h1>". "\n";
185 echo '<table style="border:1px #000000 solid">'. "\n";
186     echo '<tr>'. "\n";
187         echo '<td>Category</td>'. "\n";
188         echo '<td>Name</td>'. "\n";
189         echo '<td>Description</td>'. "\n";
190         echo '<td>Price</td>'. "\n";
191         echo '<td>Taxable</td>'. "\n";
192         // echo '<td>CpnStart</td>'. "\n";
193         // echo '<td>CpnEnd</td>'. "\n";
194         echo '<td>Hide</td>'. "\n";
195     echo '</tr>'. "\n";
196     echo '<tr>'. "\n";
197         echo '<td>
198             <select name="pCatID" form="newProductForm" >'. "\n";
199                 while($row = $catList->fetch_row()){
200                     echo '<option ';
201                     if ($row[0] == $edCatID)
202                         echo 'selected="selected" ';
203                     echo 'value="'. $row[0]. '">'. $row[1]. '</option>'. "\n";

```

```

204         }
205     echo '    </select>
206         </td>' . "\n";
207
208     echo '<form name="addProduct" action="' . $_SERVER['SCRIPT_NAME'] . '"
method="POST" id="newProductForm">';
209
210     echo '<td>
211         <input type="text"
212             name="pName"
213             required
214             title="the name of the product"
215             maxlength="32"
216             size="10"
217             value = "' . $edName . '">
218     </td>' . "\n";
219
220     echo '<td>
221         <input type="text"
222             name="pDesc"
223             title="the description of the product"
224             maxlength="256"
225             size="32"
226             value = "' . $edDesc . '">
227     </td>' . "\n";
228
229     echo '<td>
230         <input type="number"
231             name="pPrice"
232             title="price in dollars and cents"
233             pattern = "^-?\d+(\.\d{2})? $"
234             maxlength="7"
235             size="7"
236             value = "' . $edPrice . '">
237     </td>' . "\n";
238
239     echo '<td>
240         <input type="text"
241             name="pTax"
242             title="is product taxable? Y/N"
243             pattern="Y|N|y|n"
244             maxlength="1"
245             size="1"
246             value = "' . $edTax . '">
247     </td>' . "\n";
248
249     /*
250     echo '<td>
251         <input type="date"
252             name="pCstart"
253             title="coupon start date in yyyy-mm-dd"
254             pattern="^(19|20)\d\d-(0[1-9]|1[012])-(0[1-9]|[12][0-9]|3[01])$"
255             maxlength="10"
256             size="10"
257             value = "' . $edCstart . '">
258     </td>' . "\n";
259
260     echo '<td>
261         <input type="date"
262             name="pCend"

```

```

256         title="coupon end date in yyyy-mm-dd"
257         pattern="^(19|20)\d\d-(0[1-9]|1[012])-(0[1-9]|1[12][0-9]|3[01])$"
258         maxlength="10"
259         size="10"
260         value = "'. $sedCend.'">
261     </td>'."\n";*/
262     echo '<td>
263         <input type="text"
264         name="pHide"
265         title="should product be hidden from menu? Y/N"
266         pattern="Y|N|y|n"
267         maxlength="1"
268         size="1";
269         value = "'. $sedHide.'">
270     </td>'."\n";
271     echo '</tr>'."\n";
272     echo "\n". '<input type="hidden" name="posted" value="Y">';
273     echo "\n". '<input type="hidden" name="pProdID" value="'. $sedProdID.'">';
274     echo "\n". '<input type="hidden" name="filterCatID" value="'. $filterCatID.'">';
275     if ($btnEditProduct == "Edit"){
276         echo "\n". '<tr><td colspan = "8" align="center"><input type="button"
277         value="Update" onclick="validate(this.form)" >';
278         echo "\n". '<input type="hidden" name="operation" value="UPDATE">';
279     }else{
280         echo "\n". '<tr><td colspan = "8" align="center"><input type="button" value="Add
281         Product" onclick="validate(this.form)" >';
282         echo "\n". '<input type="hidden" name="operation" value="INSERT">';
283     }
284     echo "\n". '</form>';
285     echo "\n". '</table><br /><br />';
286     // Get all table (or filtered) data
287     //echo "filterCatID: ". $filterCatID. "<br />\n";
288     if(intval($filterCatID) > 0){
289         $sql = "SELECT p.* , c.NAME AS 'CATNAME'
290         FROM PRODUCTS p
291         LEFT JOIN CATEGORIES c ON p.CATID = c.CATID
292         WHERE p.CATID = '". $filterCatID.'"
293         ORDER BY CATNAME";
294     }else{
295         $sql = "SELECT p.* , c.NAME AS 'CATNAME'
296         FROM PRODUCTS p
297         LEFT JOIN CATEGORIES c ON p.CATID = c.CATID
298         ORDER BY CATNAME";
299     }
300     //echo $sql;
301     if (!( $results = $mysqli->query($sql))){
302         die("Query to show fields from table failed: $sql");
303     }
304     echo '<table><tr><td>';
305     echo '<select name="filterCatID" form="filterForm" >'."\n";
306         echo '<option value="none">None</option>';

```

```

307         $catList->data_seek(0);
308         while($row = $catList->fetch_row()){
309             echo '<option ' ;
310             if ($row[0] == $filterCatID)
311                 echo 'selected="selected" ' ;
312             echo 'value="'. $row[0]. '">'. $row[1]. '</option>' . "\n";
313         }
314     echo ' </select>' . "\n";
315     echo '</td><td>' ;
316     echo '<form name="filter" action="'. $_SERVER['SCRIPT_NAME']. '" method="POST"
id="filterForm">' . "\n";
317     echo '<input type="submit" name="btnFilter" value="Filter">' . "\n";
318     echo '</form>' . "\n";
319     echo '</td></tr></table>' ;
320
321     echo '<table style="border:1px #000000 solid" bgcolor="white">' ;
322     // $finfo = $results->fetch_fields();
323     // foreach ($finfo as $val) {
324     //     echo "<td>{$val->name}</td>";
325
326     echo "<tr>\n";
327     echo '<td>PRODID</td>' . "\n";
328     echo '<td>NAME</td>' . "\n";
329     echo '<td>CATNAME</td>' . "\n";
330     echo '<td>PRICE</td>' . "\n";
331     echo '<td>TAXABLE</td>' . "\n";
332     // echo '<td>Cpn Start</td>' . "\n";
333     // echo '<td>Cpn End</td>' . "\n";
334     echo '<td>HIDEFLAG</td>' . "\n";
335     echo "</tr>\n";
336
337     // printing table rows
338     while($row = $results->fetch_assoc())
339     {
340         echo "<tr>";
341         echo "<tr>\n";
342         echo '<td>'. $row['PRODID'] . '</td>' . "\n";
343         echo '<td><span title="'. $row['DESCRIPTION']. '"><b>'. $row['NAME']. '</b></span></td>'
. "\n";
344         echo '<td>'. $row['CATNAME'] . '</td>' . "\n";
345         echo '<td>'. number_format($row['PRICE'], 2). '</td>' . "\n";
346         echo '<td>'. (($row['TAXABLE'] == "1") ? "Y" : "N"). '</td>' . "\n";
347         // echo '<td>'. (($row['COUPONSTARTDATE'] == '0000-00-00') ? "" :
$row['COUPONSTARTDATE']). '</td>' . "\n";
348         // echo '<td>'. (($row['COUPONENDDATE'] == '0000-00-00') ? "" :
$row['COUPONENDDATE']). '</td>' . "\n";
349         echo '<td>'. (($row['HIDEFLAG'] == "1") ? "Y" : "N"). '</td>' . "\n";
350         echo '<form action="'. $_SERVER['SCRIPT_NAME']. '" method="POST">' . "\n";
351         echo '<td><input type="submit" name="btnEditProduct"
value="Edit"
></td>' . "\n";
352         echo '<td><input type="submit" name="btnDeleteProduct"
value="Delete"
></td>' . "\n";
353         echo ' <input type="hidden" name="filterCatID" value="'. $filterCatID.

```

```

    "                >'."\n";
354     echo '        <input type="hidden" name="posted"
value="Y"                >'."\n";//
355     echo '        <input type="hidden" name="edProdID"        value="' . $row['PRODID'] .
    "                >'."\n";//
356     echo '        <input type="hidden" name="edName"        value="' . $row['NAME'] .
    "                >'."\n";//
357     echo '        <input type="hidden" name="edDesc"        value="' . $row['DESCRIPTION'] .
    "                >'."\n";//
358     echo '        <input type="hidden" name="edCatID"        value="' . $row['CATID'] .
    "                >'."\n";//
359     echo '        <input type="hidden" name="edPrice"        value="' . number_format($row[
'PRICE'],2) . '">'."\n";//
360     echo '        <input type="hidden" name="edTax"        value="' . $row['TAXABLE'] .
    "                >'."\n";//
361 // echo '        <input type="hidden" name="edCstart"
value="' . $row['COUPONSTARTDATE'] . '"        >'."\n";//
362 // echo '        <input type="hidden" name="edCend"
value="' . $row['COUPONENDDATE'] . '"        >'."\n";//
363     echo '        <input type="hidden" name="edHide"        value="' . $row['HIDEFLAG'] .
    "                >'."\n";//
364     echo '        <input type="hidden" name="edCatName"        value="' . $row['CATNAME'] .
    "                >'."\n";//
365     echo "</form>";
366     echo "</tr>\n";
367 }
368 echo "</table>";
369
370 $results->close();
371 ?>
372
373
374 <!-- End
----->
----->
375         </td>
376         </tr>
377     </table>
378 </td>
379 </tr>
380 <tr height="30px" bgcolor="#FFFF00">
381     <td colspan="2">
382
383         <?php include("footer.php"); ?>
384
385     </td>
386 </tr>
387 </table>
388 </body>
389
390 </html>

```



```
1  <?php
2  if (!@session_start()){
3      die("Cannot start session");
4  }
5
6  if (!isset($_SESSION['valid_user'])){
7      //they have not tried to login, or logged out
8      echo '<script type="text/javascript"> alert("You must login first");';
9      echo 'window.location.replace("index.php"); </script>';
10     exit();
11 }
12 ?>
13
14 <html>
15 <head>
16     <title>Taste It Again - Register</title>
17 </head>
18 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"black">
19 <script type="text/javascript">
20 <!--
21 function test_it(f){
22     if((f.fName.value == '') ||
23         (f.lName.value == '') ||
24         (f.address.value == '') ||
25         (f.city.value == '') ||
26         (f.state.value == '') ||
27         (f.zipCode.value == '') ||
28         (f.email.value == '') ||
29         (f.password.value == '') ||
30         (f.password2.value == '') ||
31         (f.phone.value == '')){
32         alert("All fields must be completed.");
33         return;
34     }
35
36     if(f.password.value != f.password2.value){
37         alert("Passwords do not match.");
38         return;
39     }
40
41     f.posted.value = "OK";
42     f.submit();
43 }
44 //-->
45 </script>
46
47 <?php
48 require "mysql.php";
49
50 /*
51 //debug messages
52 echo '<pre>';
```

```

53  echo "post<br />";
54  print_r($_POST);
55  echo '</pre>';
56  */
57
58  $fName    = $_POST['fName'];
59  $lName    = $_POST['lName'];
60  $address  = $_POST['address'];
61  $address2 = $_POST['address2'];
62  $city     = $_POST['city'];
63  $state    = $_POST['state'];
64  $zipCode  = $_POST['zipCode'];
65  $email    = $_POST['email'];
66  $password = $_POST['password'];
67  $phone    = $_POST['phone'];
68  $txtflag  = ($_POST['txtflag'] == "1") ? "1":"0";
69  $mailflag = ($_POST['mailflag'] == "1") ? "1":"0";
70  $posted   = $_POST['posted'];
71  $hash     = md5($password);
72
73  if ($posted == "OK"){
74      $sql1 = "insert into USERS (EMAILADD, PWHASH, FIRSTNAME, LASTNAME, PHONE,
              CUSTFLAG)
              VALUES('$email', '$hash', '$fName', '$lName', '$phone', 'Y');"
75
76
77      $sql2 = "select USERID from USERS where EMAILADD = '$email'";
78
79      //transaction begin with implicit autocommit off
80      //echo "starting transaction<br />";
81      if (!$mysqli->query("START TRANSACTION;")){
82          echo '<script type="text/javascript">'. "\n";
83          echo 'alert("Start transaction failed: '.$mysqli->error.'");'. "\n";
84          echo 'window.back();';
85          echo '</script>'. "\n";
86          exit();
87      }
88
89      //insert into USERS table
90      //echo "inserting to USERS<br />";
91      //echo $sql1."<br />";
92      if (!$mysqli->query($sql1)){
93          //rollback
94          $err = $mysqli->error; //save error message before rollback
95          $mysqli->query("ROLLBACK;"); //must add check for rollback failure
96          echo "sql1: $sql1<br />\n";
97          echo "err: $err<br />\n";
98          echo '<script type="text/javascript">'. "\n";
99          echo 'alert("Account creation failed: '.$err.'");'. "\n";
100         echo 'window.back();';
101         echo '</script>'. "\n";
102         exit();
103     }
104

```

```

105 //retrieve auto-increment USERID
106 //echo "getting userid<br />";
107 //echo $sql2."<br />";
108 if (!( $result = $mysqli->query($sql2) )){
109     //rollback
110     $err = $mysqli->error; //save error message before rollback
111     $mysqli->query("ROLLBACK;"); //must add check for rollback failure
112     echo $sql2."<br />";
113     echo '<script type="text/javascript">'. "\n";
114     echo 'alert("Account creation failed: ' . $err . '");'. "\n";
115     echo 'window.back();';
116     echo '</script>'. "\n";
117     exit();
118 }
119
120 //echo"<pre>";
121 // print_r($result);
122 //echo"</pre>";
123
124 $row = $result->fetch_assoc();
125 $userid = $row['USERID'];
126 //echo "userid: $userid <br />";
127 $sql3 = "insert into CUSTOMERS ( USERID,  ADDLINE1,      ADDLINE2,      CITY,
STATE,      ZIP,      EMAILFLAG, TXTMSGFLAG)
128                                     VALUES($userid, '$address', '$address2', '$city', '$state
', '$zipCode', '$mailflag', '$txtflag');"
129 //echo $sql3."<br />";
130
131 //insert customer information
132 //echo "inserting CUSTOMER<br />";
133 //echo $sql3."<br />";
134 if (!$mysqli->query($sql3)){
135     $err = $mysqli->error; //save error message before rollback
136     //rollback
137     $mysqli->query("ROLLBACK;"); //must add check for rollback failure
138     echo '<script type="text/javascript">'. "\n";
139     echo 'alert("Account creation failed: ' . $err . '");'. "\n";
140     echo 'window.back();';
141     echo '</script>'. "\n";
142     exit();
143 }
144 //commit transaction
145 //echo "commting<br />";
146 if ($mysqli->query("COMMIT;")){
147     echo '<script type="text/javascript">'. "\n";
148     echo 'alert("Account created");'. "\n";
149     echo '</script>'. "\n";
150     $_SESSION['isCustomer'] = "Y";
151 }else{
152     echo '<script type="text/javascript">'. "\n";
153     echo 'alert("Commit transaction failed: ' . $mysqli->error . '");'. "\n";
154     echo 'window.back();';
155     echo '</script>'. "\n";

```

```

156         exit();
157     }
158
159 }
160 ?>
161
162 <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">
163
164     <?php include("header.php"); ?>
165
166     <tr height="500" bgcolor="#82FA58">
167         <td colspan="2">
168             <table cellspacing="0" cellpadding="0" width="900" border="0" height=
169                 "100%">
170                 <tr valign="top">
171                     <td>
172                         <!-- Start of main content
173                         ----->
174
175                         <table cellspacing="0" cellpadding="0" width="900" border=
176                             "0">
177                             <tr>
178                                 <td>
179                                     <center><h1>Register</h1></center>
180                                 </td>
181                             </tr>
182                             </table>
183                             <form name="register" id="register" action = '' method =
184                                 "post">
185                                 <table cellspacing="1" cellpadding="3" style="border:1px
186                                     #000000 solid" bgcolor="#BDBDBD" align="center">
187                                     <tr>
188                                         <td>
189                                             First Name
190                                         </td>
191                                         <td>
192                                             <input type="text" name="fName" size="20" value=
193                                                 "<?php echo $fName; ?>">
194                                         </td>
195                                     </tr>
196                                     <tr>
197                                         <td>
198                                             Last Name
199                                         </td>
200                                         <td>
201                                             <input type="text" name="lName" size="20" value=
202                                                 "<?php echo $lName; ?>">
203                                         </td>
204                                     </tr>
205                                     <tr>
206                                         <td>
207                                             Address
208                                         </td>

```

```

201         <td>
202             <input type="text" name="address" size="20"
                value="<?php echo $address; ?>">
203         </td>
204     </tr>
205     <tr>
206         <td>
207             Address Line 2
208         </td>
209         <td>
210             <input type="text" name="address2" size="20"
                value="<?php echo $address2; ?>">
211         </td>
212     </tr>
213     <tr>
214         <td>
215             City
216         </td>
217         <td>
218             <input type="text" name="city" size="20" value="
                <?php echo $city; ?>">
219         </td>
220     </tr>
221     <tr>
222         <td>
223             State
224             <input type="text" name="state" size="3" value="
                <?php echo $state; ?>">
225         </td>
226         <td>
227             Zip Code
228             <input type="text" name="zipCode" size="5" value
                ="<?php echo $zipCode; ?>">
229         </td>
230     </tr>
231     <tr>
232         <td>
233             Phone Number
234         </td>
235         <td>
236             <input type="text" name="phone" size="20" value=
                "<?php echo $phone; ?>">
237         </td>
238     </tr>
239     <tr>
240         <td>
241             Email Address
242         </td>
243         <td>
244             <input type="text" name="email" size="30" value=
                "<?php echo $email; ?>">
245         </td>
246     </tr>

```

```

247         <tr>
248             <td>
249                 Password
250             </td>
251             <td>
252                 <input type="password" name="password" size="20"
253                     value="" >
254             </td>
255         </tr>
256         <tr>
257             <td>
258                 Re-Enter Password
259             </td>
260             <td>
261                 <input type="password" name="password2" size=
262                     "20" value="">
263             </td>
264         </tr>
265         <tr>
266             <td>
267                 Send me email coupons
268             </td>
269             <td>
270                 <input type="radio" name="mailflag" value="1"
271                     <?php echo ($mailflag == "1")?"checked":""; ?> >Y
272                 <input type="radio" name="mailflag" value="0"
273                     <?php echo ($mailflag == "0")?"checked":""; ?> >N
274             </td>
275         </tr>
276         <tr>
277             <td>
278                 Send me txt message coupons
279             </td>
280             <td>
281                 <input type="radio" name="txtflag" value="1"
282                     <?php echo ($txtflag == "1")?"checked":""; ?> >Y
283                 <input type="radio" name="txtflag" value="0"
284                     <?php echo ($txtflag == "0")?"checked":""; ?> >N
285             </td>
286         </tr>
287     </table>
288     <table align="center">
289         <tr>
290             <td>
291                 <input name="btnRegister" type="button" value=
292                     "Register" onclick="test_it(this.form);"/>
293                 <input type="reset" value="Reset">
294             </td>
295         </tr>
296     </table>
297     <input name="posted" type="hidden" value="">
298 </form>
299 </td>

```

```
293         </tr>
294     </table>
295 </td>
296 </tr>
297 <tr height="30px" bgcolor="#FFFF00">
298     <td colspan="2">
299
300         <?php include("footer.php"); ?>
301
302     </td>
303 </tr>
304 </table>
305 </body>
306 </html>
307
```

```
1  <?php
2  //connect to database
3  require "mysql.php";
4
5  if (!@session_start()){
6      die("Cannot start session");
7  }
8
9  if (!isset($_SESSION['valid_user'])){
10     echo '<script type="text/javascript"> alert("You must login.");';
11     echo 'window.location.replace("index.php"); </script>';
12     exit();
13 }
14
15 /*
16 //debug messages
17 echo "<pre>";
18 echo "SESSION: <br />";
19 print_r($_SESSION);
20 echo "</pre>";
21 */
22
23 $cart = $_SESSION['cart'];
24 /*
25 //debug messages
26 echo "<pre>";
27 echo "session cart: <br />";
28 print_r($cart);
29 echo "</pre>";
30 */
31
32 //check if cart exists or is empty
33 //check cart before re-directing
34 if (count($cart) == 0){
35     echo '<script type="text/javascript"> ';
36     echo 'alert("Your cart is empty.");';
37     echo '</script>';
38 }
39
40 //get all products where $cart[key] = PRODID
41 $plist = "";
42 foreach($cart as $key => $value){
43     $plist = $plist."'.$key.'", ";
44 }
45 //remove last comma
46 $plist = substr($plist,0,strlen($plist)-2);
47 $sql = "select * from PRODUCTS where PRODID in (".$plist.") order by CATID";
48 //echo $sql."<br />";
49 if (!($menuResults = $mysqli->query($sql))){
50     die("Error - cannot get menu.\n$sql");
51 }
52
53 //get current list of all categories - created in header.php
```



```
54 $userCatList = $_SESSION['userCatList'];
55
56 /*
57 //debug messages
58 echo "<pre>";
59 echo "POST: <br/>";
60 print_r($_POST);
61 echo "</pre>";
62 */
63
64 //update cart
65 foreach($_POST as $key => $value){
66     $arr = explode("-", $key);
67     if($arr[0] == "key"){
68         //if qty = 0, delete from cart; otherwise add/update
69         if($value == 0){
70             unset($cart[$arr[1]]);
71         }else
72             $cart[$arr[1]] = $value;
73     }
74 }
75 $_SESSION['cart'] = $cart;
76
77 /*
78 //debug messages
79 echo "<pre>";
80 echo "updated cart: <br />";
81 print_r($cart);
82 echo "</pre>";
83 */
84
85 //check which, if any buttons were clicked
86 //$btnCreateUpdate = $_POST['btnCreateUpdate'];
87 //$btnCheckOut = $_POST['btnCheckOut'];
88
89
90 if(count($cart)==0)
91     $cartStatusMsg = "Order NOT created - you have 0 items in cart";
92 else{
93     $itemCount = 0;
94     foreach($cart as $key => $value){
95         $itemCount += $value;
96     }
97
98     $cartStatusMsg = "You have $itemCount items in your cart.";
99 }
100 ?>
101
102 <script type="text/javascript" >
103 function validate(f){
104     if(f.checkValidity()){
105         f.submit();
106     }else{
```

```

107     alert("Invalid data - Please check all fields");
108     return;
109 }
110 }
111 </script>
112
113 <script type="text/javascript" >
114 function viewCart(f){
115     alert("viewing cart");
116     f.action="viewcart.php";
117     alert (f.action);
118     f.submit();
119 }
120 </script>
121
122 <html>
123 <head>
124     <?php
125         if (isset($_POST['btnCheckOut'])){
126             if($_SESSION['isCustomer'] != 'Y'){
127                 echo '<script type="text/javascript"> ';
128                 echo 'alert("You must login or create an account before you can
129                     checkout.");';
130                 echo '</script>';
131             }else{
132                 //if "Check Out" button was pressed and cart is not empty, redirect to
133                 checkout.php after updating cart
134                 echo '<meta HTTP-EQUIV="REFRESH" content="0; url=checkout.php">'. "\n";
135             }
136         }
137     <?>
138
139     <title>Taste It Again - View Order</title>
140 </head>
141 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
142 "black">
143     <table cellpadding="0" cellspacing="0" width="900" align="center" border="0">
144
145         <?php include("header.php"); ?>
146
147         <tr height="500" bgcolor="#82FA58">
148             <td colspan="2">
149                 <table cellpadding="0" cellspacing="0" width="900" border="0" height=
150                     "100%">
151                     <tr valign="top">
152                         <td>
153                             <form name="menu" action="<?php echo $_SERVER['SCRIPT_NAME']
154                                 [>?>" id="menu" method = "POST">
155                             <table cellpadding="0" cellspacing="0" width="900" border=
156                                 "0">
157                                 <tr>
158                                     <?php
159                                     echo "<tr><td>$cartStatusMsg</td></tr>\n";

```

```

154      ?>
155      <td>
156          <center><h1>ORDER</h1></center>
157      </td>
158  </tr>
159  <?php
160      $currentCatID = 0;
161      $bgColor = 'white';
162
163      //print category header
164      echo ' <tr>' . "\n";
165      echo '     <td>' . "\n";
166      echo '         <table cellspacing="1" cellpadding="1"
167          style="border:1px #000000 solid" bgcolor="' . $bgColor
168          . '" align="center" width="800">' . "\n";
169      echo '             <tr>' . "\n";
170      //echo'                 <td width="150">' . "\n";
171      echo '                 <td>' . "\n";
172      echo '                 <b><h3>Category</h3></b>' .
173          "\n";
174      echo '             </td>' . "\n";
175      //echo'                 <td width="100">' . "\n";
176      echo '                 <td>' . "\n";
177      echo '                 <b><h3>Product</h3></b>' .
178          "\n";
179      echo '             </td>' . "\n";
180      //echo'                 <td width="75">' . "\n";
181      echo '                 <td>' . "\n";
182      echo '
183          <center><b><h3>Price</h3></b></center>' . "\n";
184      echo '                 </td>' . "\n";
185      //echo'                 <td width="150">' . "\n";
186      echo '                 <td>' . "\n";
187      echo '
188          <center><b><h3>Quantity</h3></b></center>' . "\n";
189      echo '                 </td>' . "\n";
190      echo '                 <td>' . "\n";
191      echo '                 <center><b><h3>Ext
192          Price</h3></b></center>' . "\n";
193      echo '                 </td>' . "\n";
194      echo '             </tr>' . "\n";
195
196      if($product = $menuResults->fetch_assoc()){ //there
197          is at least one record
198          $total = 0;
199          while (true){ //break when no more records
200              $currentCatID = intval($product['CATID']);
201              $currentCatName = $userCatList[$currentCatID
202              ];
203
204              //output new category header
205              //echo " <tr>" . "\n";
206              //echo "     <td>" . "\n";

```

```

198 //echo "          <h2>$currentCatName</h2>\n";
199 //echo "      </td>". "\n";
200 //echo "</tr>". "\n";
201
202 //alternate background colors
203 if ($bgColor != '#BDBDBD'){
204     $bgColor = '#BDBDBD';
205 }else{
206     $bgColor = 'white';
207 }
208
209 //category header was here
210
211 while (true){ //break when caetgory changes
or no more records
212     //print record
213     echo '<tr>'. "\n";
214     echo '    <td>'. "\n";
215     echo '<b>'. $currentCatName. '</b>'. "\n";
216     echo '    </td>'. "\n";
217     echo '    <td>'. "\n";
218     echo '<span title="'. $product[
'DESCRIPTION' ]. '">'. "\n";
219     echo '<b>'. $product['NAME' ]. '</b>'. "\n";
220     echo '    </td>'. "\n";
221     echo '    <td>'. "\n";
222     echo '        <center>$'. number_format(
$product['PRICE' ],2). '</center>'. "\n";
223     echo '    </td>'. "\n";
224     echo '    <td>'. "\n";
225     $pKey = 'key-'. $product['PROID'];
226     $pQty = intval($cart[$product['PROID']
]);
227     echo '        <center>
228         <input type="text"
229         name="'. $pKey. '"
230         size="2"
231         value="'. $pQty. '">
232         </center>'. "\n";
233     echo '    </td>'. "\n";
234     echo '    <td align="right">'. "\n";
235     $extprice = $pQty*$product['PRICE'];
236     $total += $extprice;
237     echo '$'. number_format($extprice,2);
238     echo '    </td>'. "\n";
239     echo '</tr>'. "\n";
240
241 //get next record
242 if (!$product = $menuResults->
fetch_assoc()){
243     //no more records
244     break;
245 }

```

```

246
247                                     //check if category changes
248                                     if (intval($product["CATID"]) !=
                                     $currentCatID){
249                                         break;
250                                     } //end if
251                                     } //end while same category
252
253                                     if (!($product)){
254                                         //no more records
255                                         break;
256                                     }
257                                     } //end while records exist
258
259                                     //print end of products table
260                                     echo'                                     <tr>
261                                         <td></td>
262                                         <td></td>
263                                         <td></td>
264                                         <td align="right">Total:</td>
265                                         <td align="right">$'.
                                         number_format($total,2).
                                         '</td>
266                                     </tr>';
267
268                                     echo'                                     </table>'."\n";
269                                     echo'                                     </td>'."\n";
270                                     echo' </tr>'."\n";
271
272                                     } //end if get record
273                                     ?>
274                                     </table>
275                                     <table align="center">
276                                         <tr>
277                                             <td>
278                                                 <?php
279                                                 if((count($cart) == 0)){//cart is empty
280                                                     echo'<input type="submit"
                                                         name="btnCreateOrder" value="Create
                                                         Order">'."\n";
281                                                     }else{
282                                                         echo'<input type="submit"
                                                         name="btnUpdateOrder" value="Update
                                                         Order">'."\n";
283                                                         echo'<input type="submit"
                                                         name="btnCheckOut" value="Check Out" >'."
                                                         \n";
284                                                         }
285                                                         ?>
286                                             </td>
287                                         </tr>
288                                     </table>
289                                     </form>

```

```
290                 </td>
291             </tr>
292         </table>
293     </td>
294 </tr>
295 <tr bgcolor="#82FA58">
296     <td colspan="2">
297         &nbsp;
298     </td>
299 </tr>
300 <tr height="30px" bgcolor="#FFFF00">
301     <td colspan="2">
302
303         <?php include( "footer.php" ); ?>
304
305     </td>
306 </tr>
307 </table>
308 </body>
309 </html>
310
```

```

1  <?php
2  //connect to database
3  require "mySQL.php";
4
5  if (!@session_start()){
6      die("Cannot start session");
7  }
8
9  if (!isset($_SESSION['valid_user'])){
10     echo '<script type="text/javascript"> alert("You must login.");';
11     echo 'window.location.replace("index.php"); </script>';
12     exit();
13 }
14
15 if(!($_SESSION['isOwner'] == 'Y')){
16     echo '<script type="text/javascript"> ';
17     echo 'alert("You must logged in as owner to view orders.");';
18     echo 'window.location = ".".$_SERVER["HTTP_REFERER"]."';
19     echo '</script>';
20     exit();
21 }
22
23 $sql = "select * from ORDERS";
24 if(!($orders = $mysqli->query($sql)){
25     die("ORDERS - could not get records.");
26 }
27 ?>
28
29 <html>
30 <head>
31     <title>Taste it Again - Home</title>
32     <?php //include("head.php"); ?>
33 </head>
34
35 <body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor=
"black">
36     <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">
37
38         <?php include("header.php"); ?>
39
40         <tr height="500" bgcolor="#82FA58">
41             <td colspan="2">
42                 <table cellspacing="0" cellpadding="0" width="900" border="0" height=
"100%">
43                     <tr valign="top">
44                         <td>
45 <!-- Start of added content
----->
46
47                 <center><h1>View Orders</h1><center>
48                 <table style="border:1px solid black" align="center" bgcolor
="white">
49                     <tr>

```

```

49         <td>Order ID</td>
50         <td>Name</td>
51         <td>Phone</td>
52         <td>Address 1</td>
53         <td>Address 2</td>
54         <td>City</td>
55         <td>State</td>
56         <td>Zip</td>
57         <td>Time</td>
58     </tr>
59     <?php
60         while($row = $orders->fetch_assoc()){
61             echo ' <tr>';
62             echo '     <td><a href="displayorder.php?ordUID='.$row[
63                 'ORDID' ].'&calledBy=owner">'.$row['ORDID' ].
64                 '</a></td>';
65             echo '     <td>'.$row['FULLNAME' ].'</td>';
66             echo '     <td>'.$row['CONTACTPHONE' ].'</td>';
67             echo '     <td>'.$row['DELADDLINE1' ].'</td>';
68             echo '     <td>'.$row['DELADDLINE2' ].'</td>';
69             echo '     <td>'.$row['DELCITY' ].'</td>';
70             echo '     <td>'.$row['DELSTATE' ].'</td>';
71             echo '     <td>'.$row['DELZIP' ].'</td>';
72             echo ' </tr>';
73         }
74     </table>
75     <!------- End of added content
----->

76         </td>
77     </tr>
78 </table>
79 </td>
80 </tr>
81 <tr height="30px" bgcolor="#FFFF00">
82     <td colspan="2">
83         <?php include("footer.php"); ?>
84     </td>
85 </tr>
86 </table>
87 </body>
88 </html>
89
90
91

```