```
<?php
//connect to database
require "mySQL.php";

if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    echo '<script type="text/javascript"> alert("You must login.");';
    echo 'window.location.replace("index.php"); </script>';
    exit();
}
?>
<html>
<head>
    <title>Taste It Again - About Us</title>
</head>

<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="gray">

    <table cellspacing="0" cellpadding="0" width="900" align="center" style="border:3px #000000 solid">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="white">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td>
                            <center><h1>About Us</h1><center>
                        </td>
                    </tr>
                    <tr>
                        <td>
                        Taste it Again, across from the Bloomfield Center redevelopment site, was started by Jacquline 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.
                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

```

```
                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>
</html>

```

```
<?php
//connect to database
require "mySQL.php";

if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    echo '<script type="text/javascript">'."\n";
    echo 'alert("You must login.");'."\n";
    echo 'window.location.replace("index.php");'."\n";
    echo '</script>'."\n";
    exit();
}
/*
echo "firstname  ".$_SESSION['firstname']."  <br/>";
echo "isAdmin    ".$_SESSION['isAdmin']."    <br/>";
echo "isOwner    ".$_SESSION['isOwner']."    <br/>";
echo "isCustomer ".$_SESSION['isCustomer']." <br/>";
echo "email      ".$_SESSION['email']."      <br/>";
*/

if($_SESSION['isAdmin'] != 'Y'){
    echo '<script type="text/javascript">'."\n";
    echo 'alert("Only administrators can use this page");'."\n";
    echo 'window.history.back();'."\n";
    echo '</script>'."\n";
    exit();
}

?>

<script type="text/javascript">
function get_name(f)
{
    f.updateFlag.value = "UPDATE";

    f.fieldData.value = prompt("Please enter the new name: ",f.fieldData.value);

    f.submit();
}
</script>

<html>
<head>
        <title>Taste it again - Category Admin</title>
    <?php //include("head.php"); ?>
</head>
<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">
    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

```

```
        <?php include("header.php"); ?>

        <tr height="500" bgcolor="#82FA58">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td><center>
<!------------ Start of main content -------------------------------------------------->
<?php
/*
echo "<pre>\n";
print_r($_POST);
echo "</pre>\n";
 */

//operation variables are the operation being performed by admin
$operation    = $_POST['operation'];     //SQL Operation UPDATE, INSERT, or DELETE
if ($_POST[updateFlag] == "UPDATE")
    $operation = "UPDATE";
$fieldData    = $_POST['fieldData'];    //data of the field being operated on
$fieldName    = $_POST['fieldName'];    //name of the field being operated on
$keyFieldData = $_POST['keyFieldData']; //primary key field name of the record being operated on
$keyFieldName = $_POST['keyFieldName']; //primary key value of the record being operated on
$table        = "CATEGORIES";

/*echo"operation    $operation   <br />\n";
echo"keyFieldData $keyFieldData<br />\n";
echo"keyFieldName $keyFieldName<br />\n";
echo"fieldData    $fieldData   <br />\n";
echo"fieldName    $fieldName   <br />\n";
echo"table        $table       <br />\n";
*/

if ($operation == "UPDATE" && $fieldName != "" && $keyFieldName != "" && $keyFieldData != "")
{
    $sql="UPDATE {$table} SET {$fieldName} = '{$fieldData}' WHERE {$keyFieldName} = '{$keyFieldData}';";
}else{
    if (($operation == "Delete") && ($keyFieldName != "") && ($keyFieldData != ""))
    {
        $sql="DELETE FROM {$table} WHERE {$keyFieldName} = '{$keyFieldData}';";
    }else{
        if (($operation == "INSERT") && ($fieldName != "") && ($fieldData != ""))
        {
            $sql="INSERT INTO {$table} ({$fieldName}) VALUES ('{$fieldData}');" ;
        }else{
            echo "Operation or values are incorrect. <br />";
        }
```

```php
    }
}

if ($sql != "")
{
    //echo "<br>attempting to run query $sql" . "<br>";
    if (!($results = $mysqli->query($sql))){
        echo("Operation query failed.<br />");
        echo("sql: $sql<br />");
    }
}

// Get whole table
$sql = "SELECT * from {$table}";
if (!($results = $mysqli->query($sql))){
    die("Query to show fields from table failed: $sql");
}
echo "<h1>Edit Table: {$table}</h1>";
echo 'You are logged in as: '.$_SESSION['valid_user'].'<br/>';
echo "\n".'<table>';
echo "\n".'<form  action="'.$_SERVER['SCRIPT_NAME'].'"  method="POST"  >';
echo "\n".'<tr><td>Enter a new Category Name: </td><td><input type="text" name="fieldData" value="" ></td></tr>';
echo "\n".'<input type="hidden" name="operation"     value="INSERT">';
echo "\n".'<input type="hidden" name="fieldName"     value="NAME">';
echo "\n".'<tr><td align="center" colspan = "2"><input type="submit" value="Add Category" >';
echo "\n".'</form>';
echo "\n".'</table>';

echo '<table style="border:1px #000000 solid" bgcolor="white"><tr>';
$finfo = $results->fetch_fields();
foreach ($finfo as $val) {
    echo "<td>{$val->name}</td>";
}
echo "</tr>\n";

// printing table rows
while($row = $results->fetch_row())
{
    echo "<tr>";

    //test comment
    foreach($row as $cell)
    echo "<td>$cell</td>";
    echo "\n".'<form action="'.$_SERVER['SCRIPT_NAME'].'" method="POST">'."\n";
    echo '<td><input type="button" name="btnChangeName" value="ChangeName" onclick="get_name(this.form);"></td>'."\n";
    echo '<td><input type="submit" name="operation"     value="Delete" >                                 </td>'."\n";
    echo '    <input type="hidden" name="keyFieldData"  value="'.$row[0].'"                                   >'."\n";//the key value of the record being operated on
    echo '    <input type="hidden" name="keyFieldName"  value="'.$finfo[0]->name.'"                           >'."\n";//the name of the key field
    echo '    <input type="hidden" name="fieldName"     value="'.$finfo[1]->name.'"                           >'."\n";//the name of the field being updated
    echo '    <input type="hidden" name="fieldData"     value="'.$row[1].'"                                   >'."\n";//holds the new name, set in get_name
    echo '    <input type="hidden" name="updateFlag" value=""                                              >'."\n";//holds the new name, set in get_name
    echo "</form>";
    echo "</tr>\n";
}
echo "</table>";

$results->close();
?>


<!-- End ------------------------------------------------------------------------------------------------------------->
                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>

</html>
```

```
<?php
if (!@session_start()){
    die("Cannot start session");
}

//check if in a valid session
if (!isset($_SESSION['valid_user'])){
    //they have not tried to login, or logged out
    echo '<script type="text/javascript">';
    echo 'alert("You must login first");';
    echo 'window.location.replace("index.php");';
    echo '</script>';
    exit();
}

$referer = $_SERVER['HTTP_REFERER'];
//check if is a customer
if ($_SESSION['isCustomer'] != 'Y'){
    echo '<script type="text/javascript"> ';
    echo 'alert("You must login or create an account before you can checkout.");';
    echo "window.location.replace(\"$referer\")";
    echo '</script>';
    exit();
}

//check if any items in cart
if (count($_SESSION['cart']) == 0){
    echo '<script type="text/javascript"> ';
    echo 'alert("Your cart is empty");';
    echo "window.location.replace(\"$referer\")";
    echo '</script>';
    exit();
}

$cart = $_SESSION['cart'];

?>

<html>
<head>
    <title>Taste It Again - Check Out</title>
</head>
<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">
<script type="text/javascript">
<!--
function test_it(f){
    if(f.checkValidity()){
        f.posted.value = "OK";
        f.submit();
    }
    else{
        alert("Please check all fields for valid data");
        return  ;
    }
}
//-->
</script>

<?php
require "mySQL.php";

/*echo '<pre>';
print_r($_POST);
echo '</pre>';*/

$posted   = $_POST['posted'];

if($posted == "OK"){
    //user attemped checkout
    $userid   = $_POST['userid'];
    $fName    = $_POST['fName'];
    $lName    = $_POST['lName'];
    $address  = $_POST['address'];
    $address2 = $_POST['address2'];
    $city     = $_POST['city'];
    $state    = $_POST['state'];
    $zipCode  = $_POST['zipCode'];
    $newemail = $_POST['email'];
    $phone    = $_POST['phone'];
    $txtflag  = $_POST['txtflag'];
    $mailflag = $_POST['mailflag'];
}else{
    $email = $_SESSION['email'];
    //load account info from database
    //get USER record
    $sql = "select * from USERS where EMAILADD = '$email';";
    //echo "sql: $sql<br />";
    if (!($results = $mysqli->query($sql))){
        die("Cannot get USER record: ".$mysqli->error);
    }
    if ($results->num_rows != 1){
        die("USERS - Wrong number of rows: ".$results->num_rows."   $sql");
    }
    $row = $results->fetch_assoc();
    $userid = $row['USERID'];
    $fName  = $row['FIRSTNAME'];
    $lName  = $row['LASTNAME'];
    $phone  = $row['PHONE'];

    //get CUSTOMER record
    $sql = "select * from CUSTOMERS where USERID = '$userid';";
    if (!($results = $mysqli->query($sql))){
        die("Cannot get CUSTOMER record: ".$mysqli->error);
    }
    if ($results->num_rows != 1){
        die("CUSTOMERS - Wrong number of rows: ".$results->num_rows);
    }
    $row = $results->fetch_assoc();
    $address  = $row['ADDLINE1'];
    $address2 = $row['ADDLINE2  '];
    $city     = $row['CITY'];
    $state    = $row['STATE'];
    $zipCode  = $row['ZIP'];
    $mailflag = $row['EMAILFLAG'];
    $txtflag  = $row['TXTMSGFLAG'];
}

if ($posted == "OK"){
    //insert new order
    $ordUID = uniqid(); //create unique ID
    $fullName = $fName." ".$lName;
    $time = date("Y-m-d H:i:s", time());

    $sql1 = "INSERT INTO `ORDERS`
            (`ORDID`  , `CUSTID` , `FULLNAME` , `CONTACTPHONE`, `DELIVERFLAG`, `DELADDLINE1`, `DELADDLINE2`, `DELCITY`, `DELSTATE`, `DELZIP`  , `TIME`)
     VALUES ('$ordUID', '$userid', '$fullName', '$phone'      ,'TRUE'         , '$address'   , '$address2'  , '$city'  , '$state'  , '$zipCode', '$time')";

    //transaction begin with implicit autocommit off
    if (!$mysqli->query("START TRANSACTION;")){
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Start transaction failed: '.$mysqli->error.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }

    //insert into ORDERS table
    if (!$mysqli->query($sql1)){
        //rollback
        $err = $mysqli->error; //save error message before rollback
        $mysqli->query("ROLLBACK;"); //must add check for rollback failure
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Account update failed: '.$err.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }

    //insert ORDERITEMS information
    $lineNum = 0;
    foreach($cart as $key=>$value){
        ++$lineNum;
        $sql2 = "insert into `ORDERITEMS`
              (`ORDID`,
               `LINENUM`,
               `QTY`,
               `EXTPRICE`,
               `NAME`,
               `PRICE`,
               `TAXABLE`)
        select
               '$ordUID' as ORDID,
               '$lineNum' as LINENUM,
               '$value' as QTY,
               ($value * PRICE) as EXTPRICE,
               NAME,
               PRICE,
               TAXABLE
        from PRODUCTS
        where PRODID = '$key'";

        echo '<script type="text/javascript">'."\n";
        echo 'alert('.$sql2.');'."\n";
        echo 'window.back();';
        echo '</script>'."\n";

        if (!$mysqli->query($sql2)){
            $err = $mysqli->error; //save error message before rollback
            //rollback
            $mysqli->query("ROLLBACK;"); //must add check for rollback failure
            echo '<script type="text/javascript">'."\n";
            echo 'alert("Account update failed: '.$err.'");'."\n";
            echo 'window.back();';
            echo '</script>'."\n";
            exit();
        }
    }//end foreach

    if (($lineNum > 0) && ($lineNum == count($cart))){ //make sure all line items were added
        //commit transaction
        if ($mysqli->query("COMMIT;")){
            unset($cart);
            unset($_SESSION['cart']);
            echo '<script type="text/javascript">'."\n";
            echo 'alert("Order Saved, confirmation sent to '.$_SESSION['email'].'");'."\n";
            echo 'window.location.replace("displayorder.php?ordUID='.$ordUID.'");';
            echo '</script>'."\n";
        }else{
            echo '<script type="text/javascript">'."\n";
            echo 'alert("Commit transaction failed: '.$mysqli->error.'");'."\n";
            echo 'window.back();';
            echo '</script>'."\n";
            exit();
        }
    }else{
        //rollback
        $mysqli->query("ROLLBACK;"); //must add check for rollback failure
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Account update failed: '.$err.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }
}
?>

    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="#82FA58">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td>
                            <table cellspacing="0" cellpadding="0" width="900" border="0">
                                <tr>
                                    <td>
                                        <center><h1>Checkout</h1></center>
                                    </td>
                                </tr>
                            </table>
                            <form name="update" id="update" action = '' method = "post">
                            <table cellspacing="1" cellpadding="3" style="border:1px #000000 solid" bgcolor="#BDBDBD" align="center">
                                <tr>
                                    <td colspan="2" align="center">
                                        <b><ul>Update Delivery Address</b></ul>
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        First Name
                                    </td>
                                    <td>
                                        <input type="text"
                                        name="fName"
                                        required
                                        size="20"
                                        value="<?php echo $fName; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Last Name
                                    </td>
                                    <td>
                                        <input type="text"
```

```
                                          name="lName"
                                          required
                                          size="20"
                                          value="<?php echo $lName; ?>">
                                      </td>
                                  </tr>
                                  <tr>
                                      <td>
                                          Address
                                      </td>
                                      <td>
                                          <input type="text"
                                          name="address"
                                          required
                                          size="20"
                                          value="<?php echo $address; ?>">
                                      </td>
                                  </tr>
                                  <tr>
                                      <td>
                                          Address Line 2
                                      </td>
                                      <td>
                                          <input type="text"
                                          name="address2"
                                          size="20"
                                          value="<?php echo $address2; ?>">
                                      </td>
                                  </tr>
                                  <tr>
                                      <td>
                                          City
                                      </td>
                                      <td>
                                          <input type="text"
                                          name="city"
                                          required
                                          size="20"
                                          value="<?php echo $city; ?>">
                                      </td>
                                  </tr>
                                  <tr>
                                      <td>
                                          State
                                          <input type="text"
                                          name="state"
                                          size="3"
                                          value="<?php echo $state; ?>">
                                      </td>
                                      <td>
                                          Zip Code
                                          <input type="text"
                                          name="zipCode"
```

```
                required
                size="5"
                value="<?php echo $zipCode; ?>">
            </td>
        </tr>
        <tr>
            <td>
                Phone Number
            </td>
            <td>
                <input type="text"
                name="phone"
                required
                size="20"
                value="<?php echo $phone; ?>">
            </td>
        </tr>
        <tr>
            <td>
                Email Address
            </td>
            <td>
                <input type="text"
                name="email" size="30"
                required
                value="<?php echo $email; ?>">
            </td>
        </tr>
        <tr>
            <td>
                Credit Card Number
            </td>
            <td>
                <input type="text"
                name="ccnum" size="30"
                required
                pattern="[A-Z]|[a-z]{16}"
                title="for this demonstration system, input 16 letters"
                maxlength="16"
                length
                value="">
            </td>
        </tr>

    </table>
    <table align="center">
        <tr>
            <td>
                <input name="btnSave" type="button" value="Checkout" onclick="test_it(this.form);"/>
                <!--<input type="reset" value="Reset">-->
            </td>
```

```
                                </tr>
                            </table>
                            <input name="posted" type="hidden" value="">
                            <input name="userid" type="hidden" value=<?php echo $userid; ?>>
                            </form>
                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>
</html>

```

```
<?php
if (!@session_start()){
    die("Cannot start session");
}

//check if in a valid session
if (!isset($_SESSION['valid_user'])){
    //they have not tried to login, or logged out
    echo '<script type="text/javascript">';
    echo 'alert("You must login first");';
    echo 'window.location.replace("index.php");';
    echo '</script>';
    exit();
}

//check if is a customer
if ($_SESSION['isCustomer'] != 'Y'){
    echo '<script type="text/javascript"> ';
    echo 'alert("You must logged in to view your order.");';
    echo '</script>';
    echo 'window.location = '."'".$_SERVER['HTTP_REFERER']."'";
    exit();
}

$ordUID = $_GET['ordUID'];
?>

<html>
<head>
    <title>Taste It Again - Check Out</title>
</head>
<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">
<script type="text/javascript">
<!--
function test_it(f){
    if(f.checkValidity()){
        f.posted.value = "OK";
        f.submit();
    }
    else{
        alert("Please check all fields for valid data");
        return  ;
    }
}
//-->
</script>

<?php
require "mySQL.php";

/*echo '<pre>';
print_r($_POST);
```

```
echo '</pre>';*/

$posted   = $_POST['posted'];

if($posted == "OK"){
    //user attemped checkout
    $userid   = $_POST['userid'];
    $fName    = $_POST['fName'];
    $lName    = $_POST['lName'];
    $address  = $_POST['address'];
    $address2 = $_POST['address2'];
    $city     = $_POST['city'];
    $state    = $_POST['state'];
    $zipCode  = $_POST['zipCode'];
    $newemail = $_POST['email'];
    $phone    = $_POST['phone'];
    $txtflag  = $_POST['txtflag'];
    $mailflag = $_POST['mailflag'];
}else{
    $email = $_SESSION['email'];
    //load account info from database
    //get USER record
    $sql = "select * from USERS where EMAILADD = '$email';";
    //echo "sql: $sql<br />";
    if (!($results = $mysqli->query($sql))){
        die("Cannot get USER record: ".$mysqli->error);
    }
    if ($results->num_rows != 1){
        die("USERS - Wrong number of rows: ".$results->num_rows."   $sql");
    }
    $row = $results->fetch_assoc();
    $userid = $row['USERID'];
    $fName  = $row['FIRSTNAME'];
    $lName  = $row['LASTNAME'];
    $phone  = $row['PHONE'];

    //get CUSTOMER record
    $sql = "select * from CUSTOMERS where USERID = '$userid';";
    if (!($results = $mysqli->query($sql))){
        die("Cannot get CUSTOMER record: ".$mysqli->error);
    }
    if ($results->num_rows != 1){
        die("CUSTOMERS - Wrong number of rows: ".$results->num_rows);
    }
    $row = $results->fetch_assoc();
    $address  = $row['ADDLINE1'];
    $address2 = $row['ADDLINE2  '];
    $city     = $row['CITY'];
    $state    = $row['STATE'];
    $zipCode  = $row['ZIP'];
    $mailflag = $row['EMAILFLAG'];
    $txtflag  = $row['TXTMSGFLAG'];
}
```

```

if ($posted == "OK"){
    //insert new order
    $ordUID = uniqid(); //create unique ID
    $fullName = $fName." ".$lName;
    $time = time();

    $sql1 = "INSERT INTO `ORDERS` 
            (`ORDID`  , `CUSTID` , `FULLNAME` , `CONTACTPHONE`, `DELIVERFLAG`,
            `DELADDLINE1`, `DELADDLINE2`, `DELCITY`, `DELSTATE`, `DELZIP`  , `TIME`)
     VALUES ('$ordUID', '$userid', '$fullName', '$phone'      ,'TRUE'         , '$address
     '   , '$address2'  , '$city'  , '$state'  , '$zipCode', $time)";

    //transaction begin with implicit autocommit off
    if (!$mysqli->query("START TRANSACTION;")){
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Start transaction failed: '.$mysqli->error.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }

    //insert into ORDERS table
    if (!$mysqli->query($sql1)){
        //rollback
        $err = $mysqli->error; //save error message before rollback
        $mysqli->query("ROLLBACK;"); //must add check for rollback failure
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Account update failed: '.$err.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }

    //insert ORDERITEMS information
    $lineNum = 0;
    foreach($cart as $key=>$value){
        echo"in loop<br />";
        ++$lineNum;
        $sql2 = "insert into `ORDERITEMS` 
              (`ORDID`, 
               `LINENUM`, 
               `QTY`, 
               `EXTPRICE`, 
               `NAME`, 
               `PRICE`, 
               `TAXABLE`) 
        select 
               '$ordUID' as ORDID, 
               '$lineNum' as LINENUM, 
               '$value' as QTY, 
               ($value * PRICE) as EXTPRICE, 
               NAME, 
               PRICE,
               TAXABLE
        from PRODUCTS
        where PRODID = '$key'";

        echo '<script type="text/javascript">'."\n";
        echo 'alert('.$sql2.');'."\n";
        echo 'window.back();';
        echo '</script>'."\n";

        if (!$mysqli->query($sql2)){
            $err = $mysqli->error; //save error message before rollback
            //rollback
            $mysqli->query("ROLLBACK;"); //must add check for rollback failure
            echo '<script type="text/javascript">'."\n";
            echo 'alert("Account update failed: '.$err.'");'."\n";
            echo 'window.back();';
            echo '</script>'."\n";
            exit();
        }
    }//end foreach

    if (($lineNum > 0) && ($lineNum == count($cart))){ //make sure all line items were added
        //commit transaction
        if ($mysqli->query("COMMIT;")){
            echo '<script type="text/javascript">'."\n";
            echo 'alert("Order Saved, confirmation sent to '.$_SESSION['email'].'");'."\n";
            echo 'window.location.replace("confrimorder.php");';
            echo '</script>'."\n";
        }else{
            echo '<script type="text/javascript">'."\n";
            echo 'alert("Commit transaction failed: '.$mysqli->error.'");'."\n";
            echo 'window.back();';
            echo '</script>'."\n";
            exit();
        }
    }else{
        //rollback
        $mysqli->query("ROLLBACK;"); //must add check for rollback failure
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Account update failed: '.$err.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }
}
?>

    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

        <?php include("header.php"); ?>
```

```

            <tr height="500" bgcolor="#82FA58">
                <td colspan="2">
                    <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                        <tr valign="top">
                            <td>
                                <table cellspacing="0" cellpadding="0" width="900" border="0">
                                    <tr>
                                        <td>
                                            <center><h1>Checkout</h1></center>
                                        </td>
                                    </tr>
                                </table>
                                <form name="update" id="update" action = '' method = "post">
                                <table cellspacing="1" cellpadding="3" style="border:1px #000000 solid" bgcolor="#BDBDBD" align="center">
                                    <tr>
                                        <td colspan="2" align="center">
                                            <b><ul>Update Delivery Address</b></ul>
                                        </td>
                                    </tr>
                                    <tr>
                                        <td>
                                            First Name
                                        </td>
                                        <td>
                                            <input type="text"
                                            name="fName"
                                            required
                                            size="20"
                                            value="<?php echo $fName; ?>">
                                        </td>
                                    </tr>
                                    <tr>
                                        <td>
                                            Last Name
                                        </td>
                                        <td>
                                            <input type="text"
                                            name="lName"
                                            required
                                            size="20"
                                            value="<?php echo $lName; ?>">
                                        </td>
                                    </tr>
                                    <tr>
                                        <td>
                                            Address
                                        </td>
                                        <td>
                                            <input type="text"
                                            name="address"
                                            required
                                            size="20"
                                            value="<?php echo $address; ?>">
                                        </td>
                                    </tr>
                                    <tr>
                                        <td>
                                            Address Line 2
                                        </td>
                                        <td>
                                            <input type="text"
                                            name="address2"
                                            size="20"
                                            value="<?php echo $address2; ?>">
                                        </td>
                                    </tr>
                                    <tr>
                                        <td>
                                            City
                                        </td>
                                        <td>
                                            <input type="text"
                                            name="city"
                                            required
                                            size="20"
                                            value="<?php echo $city; ?>">
                                        </td>
                                    </tr>
                                    <tr>
                                        <td>
                                            State
                                            <input type="text"
                                            name="state"
                                            size="3"
                                            value="<?php echo $state; ?>">
                                        </td>
                                        <td>
                                            Zip Code
                                            <input type="text"
                                            name="zipCode"
                                            required
                                            size="5"
                                            value="<?php echo $zipCode; ?>">
                                        </td>
                                    </tr>
                                    <tr>
                                        <td>
                                            Phone Number
                                        </td>
                                        <td>
                                            <input type="text"
                                            name="phone"
                                            required
                                            size="20"
                                            value="<?php echo $phone; ?>">
                                        </td>
                                    </tr>
                                    <tr>
                                        <td>
                                            Email Address
                                        </td>
                                        <td>
                                            <input type="text"
                                            name="email" size="30"
                                            required
                                            value="<?php echo $email; ?>">
                                        </td>
                                    </tr>
                                    <tr>
                                        <td>
                                            Credit Card Number
                                        </td>
                                        <td>
                                            <input type="text"
                                            name="ccnum" size="30"
                                            required
                                            pattern="[A-Z]|[a-z]{16}"
                                            title="for this demonstration system, input 16 letters"
                                            maxlength="16"
                                            length
                                            value="">
                                        </td>
                                    </tr>

                                </table>
                                <table align="center">
                                    <tr>
                                        <td>
                                            <input name="btnSave" type="button" value="Checkout" onclick="test_it(this.form);"/>
                                            <!--<input type="reset" value="Reset">-->
                                        </td>
                                    </tr>
                                </table>
                                <input name="posted" type="hidden" value="">
                                <input name="userid" type="hidden" value=<?php echo $userid; ?>>
                                </form>
                            </td>
                        </tr>
                    </table>
                </td>
            </tr>
            <tr height="30px" bgcolor="#FFFF00">
```

```
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>
</html>

```

```
<?php
//connect to database
require "mySQL.php";

if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    echo '<script type="text/javascript"> alert("You must login.");';
    echo 'window.location.replace("index.php"); </script>';
    exit();
}
?>
<html>
<head>
    <title>Taste It Again - Contact Info</title>
</head>

<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="gray">

    <table cellspacing="0" cellpadding="0" width="900" align="center" style="border:3px #000000 solid">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="white">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td>
                            <center><h1>Contact Us</h1><center>
                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>
</html>

```

```
<?php
//connect to database
require "mySQL.php";

//based on listing 23.4 in PHP book
if (!@session_start()){
    die("Cannot start session");
}

if (isset($_POST['u_id']) && isset($_POST['u_pwd'])){
    //user has just tried to log in
    $u_id = $_POST['u_id'];
    $u_pwd = $_POST['u_pwd'];


    $query = "select * from CPANELUSERS where USERID = '$u_id' and PWHASH = '".md5($u_pwd)."'";
    $result = $mysqli->query($query);
    if ($result->num_rows){
        //if they are in the dataabse, register the user id and privleges
        $_SESSION['valid_user'] = $u_id;
        $row = $result->fetch_assoc();
        $_SESSION['cpanel_admin'] = $row['ADMINFLAG'];
        $result->close();
    }
    else{
        unset($_SESSION['valid_user']);
        unset($_SESSION['cpanel_admin']);
        echo '<script type="text/javascript"> alert("Invalid username/password");';
        echo 'window.history.back(); </script>';
        exit();
    }
}
?>

<html><head>
<title>Edit CPanel Users</title>
</head>

<body>
<script type="text/javascript" >

function get_pw(f)
{
    f.op_ChangePW.value = "ChangePW";

    if (f.operation_id.value == "")
    {
        alert("Error - no user account selected.");
        return;
    }

    f.operation_pwd.value = prompt("Please enter the new password: ","");

    if (f.operation_pwd.value != prompt("Please re-enter the new password: ",""))
    {
        alert("Passwords do not match.");
        return;
    }

    f.submit();
}
</script>

<script type="text/javascript" >
function test_it(f)
{
    if (f.operation_id.value == ""   || f.operation_pwd.value == "")
    {
       alert("You have to enter a user ID and password!");
       return;
    }

    if (f.operation_pwd.value != f.operation_pwd2.value)
    {
       alert("Passwords do not match");
       return;
    }

    //changes to catch XSS and SQL injection
    if ((f.operation_id.value.indexOf("<") != -1) || (f.operation_pwd.value.indexOf("<") != -1) ||
    (f.operation_id.value.indexOf("'") != -1) || (f.operation_pwd.value.indexOf("'") != -1))
    {
    alert("You have illegal characters in user ID or password!");
    return;
    }

   //alert(f.operation_id.value + ' ' + f.operation_pwd.value ) ;
   f.submit();

}

</script>
<?php
    if (isset($_SESSION['valid_user'])){
        //echo 'You are logged in as: '.$_SESSION['valid_user'].'<br/>';
        //echo '<a href="cPanelLogout.php">Log out</a><br />';
}else{
    if(isset($u_id)){
        //they tied and failed to login
        echo '<script type="text/javascript"> alert("Invalid username/password");';
        echo 'window.history.back(); </script>';
    }else{
        //they have not tried to login, or logged out
        echo '<script type="text/javascript"> alert("You must login first");';
        echo 'window.location.replace("index.php"); </script>';
        exit();
    }
}

?>

<?php

//operation variables are the operation being performed by cpanel admin
$op_NewUser      = ($_POST['op_NewUser']  == "NewUser")  ? "TRUE" : "FALSE";
$op_ChangePW     = ($_POST['op_ChangePW'] == "ChangePW") ? "TRUE" : "FALSE";
$op_AdminOn      = ($_POST['op_AdminOn']  == "AdminOn")  ? "TRUE" : "FALSE";
$op_AdminOff     = ($_POST['op_AdminOff'] == "AdminOff") ? "TRUE" : "FALSE";
$op_Delete       = ($_POST['op_Delete']   == "Delete")   ? "TRUE" : "FALSE";
$operation_id    = $_POST['operation_id'] ;
$operation_pwd   = $_POST['operation_pwd'];
$operation_hash  = md5($operation_pwd);
$operation_admin = empty($_POST['operation_admin']) ? 'FALSE' : $_POST['operation_admin'];
$table           = "CPANELUSERS";

if (!($_SESSION['cpanel_admin']=='1')){
    echo '<script type="text/javascript"> window.location.replace("home.php") </script>';
    exit;
}

if ($op_ChangePW == "TRUE" && $operation_id != "")
{
    $sql="UPDATE {$table} SET PWHASH = '{$operation_hash}' WHERE USERID = '{$operation_id}';";
}

if ($op_Delete == "TRUE" && $operation_id != "")
{
    $sql="DELETE FROM {$table} WHERE USERID = '{$operation_id}';";
}

if ($op_AdminOn == "TRUE" && $operation_id != "")
{
    $sql="UPDATE {$table} SET ADMINFLAG = TRUE WHERE USERID = '{$operation_id}';";
}

if ($op_AdminOff == "TRUE" && $operation_id != "")
{
    $sql="UPDATE {$table} SET ADMINFLAG = FALSE WHERE USERID = '{$operation_id}';";
}

if ($op_NewUser == "TRUE" && $operation_id != "" && $operation_hash != "" )
{
    $sql="INSERT INTO {$table} VALUES ('{$operation_id}', '{$operation_hash}', {$operation_admin});" ;
```

```
}

if ($sql != "")
{
    //echo "<br>attempting to run query $sql" . "<br>";
    if (!($results = $mysqli->query($sql))){
        echo("Operation query failed.");
    }
}

// sending query
$sql = "SELECT * from {$table}";
if (!($results = $mysqli->query($sql))){
    die("Query to show fields from table failed: $sql");
}
echo "<h1>Edit Table: {$table}</h1>";
echo 'You are logged in as: '.$_SESSION['valid_user'].'<br/>';
echo "\n".'<table>';
echo "\n".'<form  action="'.$_SERVER['SCRIPT_NAME'].'"  method="POST"  >';
echo "\n".'<tr><td>Enter a new userID: </td><td><input type="text" name="operation_id"
value="" ></td></tr>';
echo "\n".'<tr><td>Enter a password: </td><td><input type="password"
name="operation_pwd" value=""></td></tr>';
echo "\n".'<tr><td>Re-enter password: </td><td><input type="password"
name="operation_pwd2" value=""></td></tr>';
echo "\n".'<tr><td colspan = "2">Admin?';
echo "\n".'<input type="radio" name="operation_admin" value="TRUE"> Y';
echo "\n".'<input type="radio" name="operation_admin" value="FALSE" checked>
N</td></tr>';
echo "\n".'<input type="hidden" name="op_NewUser"     value="NewUser">';
echo "\n".'<tr><td colspan = "2"><input type="button" value="Add ID"
onclick="test_it(this.form);" >';
echo "\n".'<input type="button" value="Homepage" onclick="location.href='."'home.php'".
'" >';
echo "\n".'<input type="button" value="Logout" onclick="location.href='.
"'cPanelLogout.php'".'" >';
echo "\n".'<input type="button" value="View Development Log" onclick="window.open('.
"'http://blue.cs.montclair.edu/~cmpt483a/dev/~DevLog.txt'".');"  >';
echo '</td></tr>';
echo "\n".'</form>';
echo "\n".'</table>';

echo "<table border='1'><tr>";
$finfo = $results->fetch_fields();
foreach ($finfo as $val) {
    echo "<td>{$val->name}</td>";
}
echo "</tr>\n";

// printing table rows
while($row = $results->fetch_row())
{
    echo "<tr>";

    //test comment
    foreach($row as $cell)
    echo "<td>$cell</td>";
    echo "\n".'<form action="'.$_SERVER['SCRIPT_NAME'].'" method="POST">'."\n";
    echo '<td><input type="button" name="btnChangePW"   value="ChangePW"
    onclick="get_pw(this.form);"></td>'."\n";
    echo '<td><input type="submit" name="op_AdminOn"    value="AdminOn" ></td>'."\n";
    echo '<td><input type="submit" name="op_AdminOff"   value="AdminOff"></td>'."\n";
    echo '<td><input type="submit" name="op_Delete"     value="Delete"  ></td>'."\n";
    echo '    <input type="hidden" name="op_ChangePW"   value=""             >'."\n";
    //the flag for changing password
    echo '    <input type="hidden" name="operation_id"  value="'.$row[0].'"  >'."\n";
    //the user id being operated on
    echo '    <input type="hidden" name="operation_pwd" value="FALSE"        >'."\n";
    //holds the new password, set in get_pw
    echo "</form>";
    echo "</tr>\n";
}
echo "</table>";

$results->close();
?>



</body></html>
```

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

```
<?php
if (!@session_start()){
    die("Cannot start session");
}

//check if in a valid session
if (!isset($_SESSION['valid_user'])){
    //they have not tried to login, or logged out
    echo '<script type="text/javascript">';
    echo 'alert("You must login first");';
    echo 'window.location.replace("index.php");';
    echo '</script>';
    exit();
}

//check if is a customer
if (($_SESSION['isCustomer'] != 'Y') && ($_SESSION['isOwner'] != 'Y')){
    echo '<script type="text/javascript"> ';
    echo 'alert("You must logged in as customer or owner to view orders.");';
    echo 'window.location = '."'".$_SERVER['HTTP_REFERER']."'";
    echo '</script>';
    exit();
}

$ordUID = $_GET['ordUID'];
if ($ordUID == ''){
    echo '<script type="text/javascript"> ';
    echo 'alert("Error - invalid order ID: '.$ordUID.'");';
    echo 'window.location = '."'".$_SERVER['HTTP_REFERER']."'";
    echo '</script>';
    exit();
}

//changes function of button at the bottom
$calledBy = $_GET['calledBy'];

?>

<html>
<head>
    <title>Taste It Again - Display Order</title>
</head>
<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">
<script type="text/javascript">
<!--
function test_it(f){
    if(f.checkValidity()){
        f.posted.value = "OK";
        f.submit();
    }
    else{
        alert("Please check all fields for valid data");
        return  ;
    }
}
//-->
</script>

<?php
require "mySQL.php";

/*echo '<pre>';
print_r($_POST);
echo '</pre>';*/


//load ORDERS record info from database
$sql = "select * from ORDERS where ORDID = '$ordUID';";
//echo "sql: $sql<br />";
if (!($results = $mysqli->query($sql))){
    die("Cannot get ORDERS record: ".$mysqli->error);
}
if ($results->num_rows != 1){
    die("ORDERS - Wrong number of rows: ".$results->num_rows."  $sql");
}
$order = $results->fetch_assoc();

$sql = "select * from ORDERITEMS where ORDID = '$ordUID'";
if (!($lineitems = $mysqli->query($sql))){
    die("ORDERITEMS - Cannot get records");
}
?>

    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="#82FA58">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td>
                            <table cellspacing="0" cellpadding="0" width="900" border="0">
                                <tr>
                                    <td>
                                        <center><h1>Order Confirmation</h1></center>
                                    </td>
                                </tr>
                            </table>
                            <table cellspacing="1" cellpadding="3" style="border:1px #000000 solid" bgcolor="white" align="center">
                                <tr>
                                    <td colspan="2" align="center">
```

```
                                        <b><ul>Delivery Address</b></ul>
                                    </td>
                                </tr>
                                <tr>
                                    <td>Full Name</td>
                                    <td><?php echo $order['FULLNAME']; ?></td>
                                </tr>
                                <tr>
                                    <td>Address</td>
                                    <td><?php echo $order['DELADDLINE1']; ?></td>
                                </tr>
                                <tr>
                                    <td>Address Line 2</td>
                                    <td><?php echo $order['DELADDLINE2']; ?></td>
                                </tr>
                                <tr>
                                    <td>City</td>
                                    <td><?php echo $order['DELCITY']; ?></td>
                                </tr>
                                <tr>
                                    <td>State</td>
                                    <td><?php echo $order['DELSTATE']; ?></td>
                                </tr>
                                <tr>
                                    <td>Zip Code</td>
                                    <td><?php echo $order['DELZIP']; ?></td>

                                </tr>
                                <tr>
                                    <td>Phone Number</td>
                                    <td><?php echo $order['CONTACTPHONE']; ?></td>
                                </tr>
                                <tr>
                                    <td>Time Posted</td>
                                    <td><?php echo $order['TIME']; ?></td>
                                </tr>
                            </table>
                            <table align="center">
                                <tr>
                                    <td>
                                    <?php
                                        if ($calledBy == '')
                                            echo"<input type=\"button\" value=\"Home\" onclick=\"location.href='home.php'\" >";
                                        else
                                            echo"<input type=\"button\" value=\"Return\" onclick=\"window.history.back()\" >";
                                    ?>
                                    </td>
                                </tr>
                            </table>
                    <table style="border:1px #000000 solid" align="center" bgcolor=
                    "white">
                        <tr>
                            <td><b>#</b></td><td><b>Name</b></td><td><b>Price
                            </b></td><td><b>Taxable</b></td><td><b>Qty</b></td><td><b>
                            Ext Price</b></td>
                        </tr>
                        <?php

                        $total = 0;
                        while($row = $lineitems->fetch_assoc() ){
                            echo'<tr>';
                            echo'   <td>'.$row['LINENUM'].'</td>';
                            echo'   <td>'.$row['NAME'].'</td>';
                            echo'   <td align="right">'.number_format($row['PRICE'],2).
                            '</td>';
                            echo'   <td align="center">'.$row['TAXABLE'].'</td>';
                            echo'   <td align="center">'.$row['QTY'].'</td>';
                            echo'   <td align="right">'.number_format($row['EXTPRICE'],2
                            ).'</td>';
                            echo'</tr>';
                            $total += $row['EXTPRICE'];
                        }
                        echo'<tr><td></td><td></td><td></td><td></td><td
                        align="right"><b>Total:</b></td><td align="right">'.
                        number_format($total,2).'</td></tr>';
                        ?>
                    </table>
                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>
</html>

```

```
<?php
if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    //they have not tried to login, or logged out
    echo '<script type="text/javascript"> alert("You must login first");';
    echo 'window.location.replace("index.php"); </script>';
    exit();
}
?>

<html>
<head>
    <title>Taste It Again - Edit Account</title>
</head>
<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">
<script type="text/javascript">
<!--
function test_it(f){
    if((f.fName.value == '') ||
        (f.lName.value == '') ||
        (f.address.value == '') ||
        (f.city.value == '') ||
        (f.state.value == '') ||
        (f.zipCode.value == '') ||
        (f.email.value == '') ||
        (f.phone.value == '')){
            alert("All fields must be completed.");
            return;
        }

        f.posted.value = "OK";
        f.submit();
}
//-->
</script>

<?php
require "mySQL.php";

/*echo '<pre>';
print_r($_POST);
echo '</pre>';*/

$posted   = $_POST['posted'];

if($posted == "OK"){
    //user attemped update
    $userid   = $_POST['userid'];
    $fName    = $_POST['fName'];
    $lName    = $_POST['lName'];
    $address  = $_POST['address'];
    $address2 = $_POST['address2'];
    $city     = $_POST['city'];
    $state    = $_POST['state'];
    $zipCode  = $_POST['zipCode'];
    $newemail = $_POST['email'];
    $phone    = $_POST['phone'];
    $txtflag  = $_POST['txtflag'];
    $mailflag = $_POST['mailflag'];
}else{
    $email = $_SESSION['email'];
    //load account info from database
    //get USER record
    $sql = "select * from USERS where EMAILADD = '$email';";
    //echo "sql: $sql<br />";
    if (!($results = $mysqli->query($sql))){
        die("Cannot get USER record: ".$mysqli->error);
    }
    if ($results->num_rows != 1){
        die("USERS - Wrong number of rows: ".$results->num_rows."   $sql");
    }
    $row = $results->fetch_assoc();
    $userid = $row['USERID'];
    $fName  = $row['FIRSTNAME'];
    $lName  = $row['LASTNAME'];
    $phone  = $row['PHONE'];

    //get CUSTOMER record
    $sql = "select * from CUSTOMERS where USERID = '$userid';";
    if (!($results = $mysqli->query($sql))){
        die("Cannot get CUSTOMER record: ".$mysqli->error);
    }
    if ($results->num_rows != 1){
        die("CUSTOMERS - Wrong number of rows: ".$results->num_rows);
    }
    $row = $results->fetch_assoc();
    $address  = $row['ADDLINE1'];
    $address2 = $row['ADDLINE2'];
    $city     = $row['CITY'];
    $state    = $row['STATE'];
    $zipCode  = $row['ZIP'];
    $mailflag = $row['EMAILFLAG'];
    $txtflag  = $row['TXTMSGFLAG'];
}

if ($posted == "OK"){
    $sql1 = "UPDATE USERS SET
        EMAILADD   = '$newemail',
        FIRSTNAME  = '$fName',
        LASTNAME   = '$lName',
        PHONE      = '$phone'
        WHERE USERID = '$userid';";

    $sql2 = "UPDATE CUSTOMERS SET
        ADDLINE1   = '$address',
        ADDLINE2   = '$address2',
        CITY       = '$city',
        STATE      = '$state',
        ZIP        = '$zipCode',
        EMAILFLAG  = '$mailflag',
        TXTMSGFLAG = '$txtflag'
        WHERE USERID = '$userid';";

    //transaction begin with implicit autocommit off
    if (!$mysqli->query("START TRANSACTION;")){
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Start transaction failed: '.$mysqli->error.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }

    //insert into USERS table
    if (!$mysqli->query($sql1)){
        //rollback
        $err = $mysqli->error; //save error message before rollback
        $mysqli->query("ROLLBACK;"); //must add check for rollback failure
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Account update failed: '.$err.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }

    //insert customer information
    if (!$mysqli->query($sql2)){
        $err = $mysqli->error; //save error message before rollback
        //rollback
        $mysqli->query("ROLLBACK;"); //must add check for rollback failure
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Account update failed: '.$err.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }
    //commit transaction
    if ($mysqli->query("COMMIT;")){
        $_SESSION['email'] = $newemail;
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Account updated");'."\n";
        echo 'window.location.replace("home.php");';
        echo '</script>'."\n";
    }else{
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Commit transaction failed: '.$mysqli->error.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }

}
?>

    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="#82FA58">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td>
<!------------ Start of main content --------------------------------------------------------------------------------------->

                            <table cellspacing="0" cellpadding="0" width="900" border="0">
                                <tr>
                                    <td>
                                        <center><h1>Register</h1></center>
                                    </td>
                                </tr>
                            </table>
                            <form name="update" id="update" action = '' method = "post">
                            <table cellspacing="1" cellpadding="3" style="border:1px #000000 solid" bgcolor="#BDBDBD" align="center">
                                <tr>
                                    <td>
                                        First Name
                                    </td>
                                    <td>
                                        <input type="text" name="fName" size="20" value="<?php echo $fName; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Last Name
                                    </td>
                                    <td>
                                        <input type="text" name="lName" size="20" value="<?php echo $lName; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Address
                                    </td>
                                    <td>
                                        <input type="text" name="address" size="20" value="<?php echo $address; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Address Line 2
                                    </td>
                                    <td>
                                        <input type="text" name="address2" size="20" value="<?php echo $address2; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        City
                                    </td>
                                    <td>
                                        <input type="text" name="city" size="20" value="<?php echo $city; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        State
                                        <input type="text" name="state" size="3" value="<?php echo $state; ?>">
                                    </td>
                                    <td>
                                        Zip Code
                                        <input type="text" name="zipCode" size="5" value="<?php echo $zipCode; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Phone Number
                                    </td>
                                    <td>
                                        <input type="text" name="phone" size="20" value="<?php echo $phone; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Email Address
                                    </td>
                                    <td>
                                        <input type="text" name="email" size="30" value="<?php echo $email; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Send me email coupons
                                    </td>
                                    <td>
                                        <input type="radio" name="mailflag" value="1" <?php echo ($mailflag == "1")?"checked":""; ?> >Y
                                        <input type="radio" name="mailflag" value="0" <?php echo ($mailflag == "0")?"checked":""; ?> >N
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Send me txt message coupons
                                    </td>
                                    <td>
                                        <input type="radio" name="txtflag" value="1" <?php echo ($txtflag == "1")?"checked":""; ?> >Y
                                        <input type="radio" name="txtflag" value="0" <?php echo ($txtflag == "0")?"checked":""; ?> >N
                                    </td>
                                </tr>
                            </table>
                            <table align="center">
                                <tr>
                                    <td>
                                        <input name="btnSave" type="button" value="Save Changes" onclick="test_it(this.form);"/>
                                        <!--<input type="reset" value="Reset">-->
                                    </td>
                                </tr>
                            </table>
                            <input name="posted" type="hidden" value="">
                            <input name="userid" type="hidden" value=<?php echo $userid; ?>>
                            </form>
                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>
</html>

```

```
<table cellspacing="0" cellpadding="0" width="900" border="0">
    <tr>
        <td>
            <center><font color="#04B404"><B>Copyright Info</B></font></center>
        </td>
    </tr>
</table>
```

```

<style type="text/css">
.nav a:link {color:#04B404; text-decoration:none; font-family: arial black; font-weight: bold}
.nav a:visited {color:#04B404; font-family: arial black; font-weight: bold}
.nav a:hover {text-decoration:none; color:#000000; font-family: arial black; font-weight: bold}
.nav a:active {font-family: arial black; font-weight: bold}

.header a:link {color:#04B404; text-decoration:none;}
.header a:visited {color:#04B404;}
.header a:hover {text-decoration:underline;}
.header a:active {}

.vieworder a:link {color:#FFFF00; text-decoration:; font-weight: bold;}
.vieworder a:visited {color:#FFFF00;}
.vieworder a:hover {text-decoration:; color:#000000}
.vieworder a:active {}

.button_link a:link {text-decoration:none;}
.button_link a:visited {}
.button_link a:hover {text-decoration:none;}
.button_link a:active {}

.welcome {
    color: #FFFF00;
    font-family: verdana;
    font-size: 12px;
}
</style>

<?php
$firstname  = $_SESSION['firstname'];
$firstname  = ($firstname == '')?"Guest":$firstname;
$isAdmin    = $_SESSION['isAdmin'];
$isOwner    = $_SESSION['isOwner'];
$isCustomer = $_SESSION['isCustomer'];
$email      = $_SESSION['email'];

//unset($_SESSION['userCatList']);
//get category list for users (Admin users have a real-time category list when administering categories and products)
if (!isset($_SESSION['userCatList'])){
    if ($result = @$mysqli->query("select CATID, NAME from CATEGORIES")){
        $userCatList = array();
        while ($row = $result->fetch_assoc()){
            $userCatList[intval($row['CATID'])] = $row['NAME'];
        }
        $_SESSION['userCatList'] = $userCatList;
    }else{
        echo '<script type="text/javascript"> alert("Error - cannot get category list: ' .$mysqli->error.'");</script>';
    }
```

```
}else{
    $userCatList = $_SESSION['userCatList'];
    /*
    echo "<pre>";
    print_r($userCatList);
    echo "</pre>";*/
}

?>
<link rel="stylesheet" href="styles.css" type="text/css">
        <tr height="100px" bgcolor="#04B404">
            <td>
                <table cellspacing="0" cellpadding="0" align="center" border="0">
                    <tr align="center">
                        <td align="center">
                            <center><font color="#FFFF00" face="arial black"><h1>T a s t e &nbsp; I t &nbsp; A g a i n</h1></font></center>
                        </td>
                    </tr>
                    <tr>
                        <td>
                            <center><font face="fantasy" color="#FFFF00">- F i n e &nbsp; J a m a i c a n &nbsp; D i n i n g - </font></center><br />
<!--                            271 Glenwood Avenue Bloomfield, NJ 07003<br />
                            Phone: (973)743-5140
-->
                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr width="100%" height="30px" bgcolor="#FFFF00">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" bgcolor="#FFFF00">
                    <tr>
                        <div id='cssmenu'>
                            <ul>
                                <li class='active '><a href='home.php'><span>HOME</span></a></li>
                                <li class='has-sub '><a href='menu.php?cat=000000'><span>MENU</span></a>
                                    <ul>
                                        <li><a href="menu.php?cat=000000">All Menu Items </a></li>
                                        <?php
                                        foreach ($userCatList as $key => $value){
                                            if ($value != "Merchandise"){ //merchandise has its own menu
                                                echo '<li><a href="menu.php?cat='.$key.'">'.$value.'</a></li>'."\n";
                                            }
                                        }
                                        ?>
                                    </ul>
                                </li>
                                <li><a href='merch.php'><span>MERCHANDISE</span></a></li>
                                <li><a href='info.php'><span>INFORMATION</span></a></li>
                            </ul>
                        </div>
                    </tr>
                </table>
            </td>
        </tr>
        <tr width="100%" height="25px" bgcolor="#40FF00">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" bgcolor="#04B404">
                    <tr>
                        <td>
                            <span class="welcome">
                                &nbsp; Welcome, <?php echo $firstname; ?>!
                                <?php
                                    if (count($_SESSION['cart']) > 0){
                                        echo '<span class="welcome"> | </span><span class="vieworder"><a href="viewcart.php">View Order</a></span>';
                                    }
                                ?>
                            </span>

<!--
                            <?php
                                if($isCustomer == 'Y'){
                                    echo 'CUSTOMER = YES';
                                }else{
                                    echo 'CUSTOMER = NO';
                                }
                            ?>
-->

                        </td>
                        <form name="login" id="login" action="homelogin.php" method="POST">
                        <td align="right">
                            <span class="welcome">
                                Email <input type="text" name="email" size="20">
                                Password <input type="password" name="password" size="20">
                            </span>
                            <?php
                                if (!($isCustomer == 'Y')){
                                    echo '<input type="submit" value="Login">';
                                }else{
                                    echo '<span class="button_link"><a
                                    href="homelogout.php"><input type="button" value="Logout"></a></span>';
                                }
                            ?>
                            <?php
                                if ($isCustomer == 'Y'){
                                    echo '<span class="button_link"><a href="editAccount.php"><input type="button" value="Edit Account"></a></span>';
                                }else{
                                    echo '<span class="button_link"><a href="register.php"><input type="button" value="Register"></a></span>';
                                }
                            ?>
                        </td>
                        </form>
                    </tr>
                </table>
            </td>
        </tr>
    <?php
        if(($isAdmin =='Y')){
            echo '<tr width="100%" height="25px" bgcolor="#40FF00">';
            echo '  <td colspan="2">';
            echo '      <table cellspacing="0" cellpadding="0" width="900" border="0" bgcolor="#04B404">';
            echo '          <tr>';
            echo '              <td align="left">';
            echo '                  <span class="welcome">';
            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>';
            echo '                  </span>';
            echo '              </td>';
            echo '          </tr>';
            echo '      </table>';
            echo '  </td>';
            echo '</tr>';
        }
    ?>

    <?php
        if(($isOwner =='Y')){
            echo '<tr width="100%" height="25px" bgcolor="#40FF00">';
            echo '  <td colspan="2">';
            echo '      <table cellspacing="0" cellpadding="0" width="900" border="0" bgcolor="#04B404">';
            echo '          <tr>';
            echo '              <td align="left">';
            echo '                  <span class="welcome">';
            echo '                      &nbsp; <b>- Owner Menu -</b> &nbsp;<span
            class="button_link"><a href="vieworders.php"><input type="button"
            value="View Orders"></a></span>';
            echo '                  </span>';
            echo '              </td>';
            echo '          </tr>';
            echo '      </table>';
            echo '  </td>';
            echo '</tr>';
        }
    ?>
```

```
<?php
//connect to database
require "mySQL.php";

if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    echo '<script type="text/javascript"> alert("You must login.");';
    echo 'window.location.replace("index.php"); </script>';
    exit();
}

?>

<html>
<head>
    <title>Taste it Again - Home</title>
    <?php //include("head.php"); ?>
</head>

<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">

    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="#82FA58">
            <td colspan="2">
<!------------ Start of main content -------------------------------------------->

                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr height="20">
                        <td>&nbsp;
                        </td>
                    </tr>
                    <tr valign="top">
                        <td align="center">
                            <img src="images/flag.png" border="0">
                        </td>
                        <td colspan="3">
                            Welcome to Taste It Again!  Here, you can experience the fine cuisine of Jamaica, without actually being there.
                        </td>
                    </tr>
                    <tr>
                        <td>
                            <img src="images/food1.jpg" border="0" height="300" width="300">
                        </td>
                        <td>
                            <img src="images/food2.jpg" border="0" height="300" width="300">
                        </td>
                        <td>
                            <img src="images/food3.jpg" border="0" height="300" width="300">
                        </td>
                    </tr>
                </table>
<!------------- End of added content -------------------------------------------->
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>
</html>

```

```php
<?php
include "mySQL.php";

if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    //they have not tried to login, or logged out
    echo '<script type="text/javascript"> alert("You must login first");';
    echo 'window.location.replace("index.php"); </script>';
    exit();
}

$email = strtolower($_POST['email']);
$password = $_POST['password'];
$hash = md5($password);

if (!$results = $mysqli->query("SELECT * from USERS where EMAILADD = '$email' AND PWHASH = '$hash'")){
    die("Query failed");
}
if ($results->num_rows > 1){
    die("Query error - too many rows returned.");
}

$row = $results->fetch_assoc();
if (!$row){
    echo '<script type="text/javascript"> alert("Invalid username/password");';
    echo 'window.location = '."'".$_SERVER['HTTP_REFERER']."'";
    echo '</script>';
    exit();
}

$_SESSION['firstname']  = $row['FIRSTNAME'];
$_SESSION['isAdmin']    = $row['ADMINFLAG'];
$_SESSION['isOwner']    = $row['OWNERFLAG'];
$_SESSION['isCustomer'] = $row['CUSTFLAG'];
$_SESSION['email']      = $email;

/*
//debug messages
echo "firstname  ".$_SESSION['firstname']."  <br/>";
echo "isAdmin    ".$_SESSION['isAdmin']."    <br/>";
echo "isOwner    ".$_SESSION['isOwner']."    <br/>";
echo "isCustomer ".$_SESSION['isCustomer']." <br/>";
echo "email      ".$_SESSION['email']."      <br/>";
*/

echo '<script type="text/javascript">';
echo 'alert("Login Successful");';
echo 'window.location = '."'".$_SERVER['HTTP_REFERER']."'";
echo '</script>';
```

```
?>
```

```php
<?php
include "mySQL.php";

if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    //they have not tried to login, or logged out
    echo '<script type="text/javascript"> alert("You must login first");';
    echo 'window.location.replace("index.php"); </script>';
    exit();
}
//echo '<pre>';
//print_r($_SESSION);
//echo '</pre>';

unset($_SESSION['email']);
unset($_SESSION['firstname']);
unset($_SESSION['isAdmin']);
unset($_SESSION['isOwner']);
unset($_SESSION['isCustomer']);

echo '<script type="text/javascript">';
echo 'alert("You have been logged out.");';
echo 'window.location = '."'home.php'";
echo '</script>';

?>
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
<meta content="text/html; charset=utf-8" http-equiv="Content-Type" />
<title>Create Account</title>
<style type="text/css">
.auto-style1 {
    text-align: right;
}
</style>
</head>

<body>

<script type="text/javascript">
<!--
function test_it(f){
    if((f.fName.value == '') ||
        (f.lName.value == '') ||
        (f.email.value == '') ||
        (f.password.value == '') ||
        (f.password2.value == '') ||
        (f.phone.value == '')){
            alert("All fields must be completed.");
            return;
        }

        if(f.password.value != f.password2.value){
            alert("Passwords do not match.");
            return;
        }
        f.posted.value = "OK";
        f.submit();
}
//-->
</script>

<?php
require "mySQL.php";
$fName    = $_POST['fName'];
$lName    = $_POST['lName'];
$email    = $_POST['email'];
$password = $_POST['password'];
$phone    = $_POST['phone'];
$posted   = $_POST['posted'];
$hash     = md5($password);

echo "<br>posted: $posted";

if ($posted == "OK"){
    $sql = "insert into USERS (EMAILADD, PWHASH, FIRSTNAME, LASTNAME, PHONE) VALUES('
    $email', '$hash', '$fName', '$lName','$phone');";
    echo "<br>sql: $sql";

    if($result = $mysqli->query($sql)){
        echo '<script type="text/javascript"> alert("Account created"); </script>';
    }else{
        //echo '<script type="text/javascript"> alert("Account creation failed: 
        "+$mysqli->error); </script>';
        echo '<script type="text/javascript"> alert($mysqli->error); </script>';
    }


}
?>

<h1>Create Account</h1>
<table>
<form action="" method="post">
    <tr><td class="auto-style1">First Name:        </td><td> <input name="fName" 
    type="text"     value="<?php echo $fName; ?>" /></td></tr>
    <tr><td class="auto-style1">Last Name:         </td><td> <input name="lName" 
    type="text"     value="<?php echo $lName; ?>" /></td></tr>
    <tr><td class="auto-style1">E-Mail Address:    </td><td> <input name="email" 
    type="text"     value="<?php echo $email ?>" /></td></tr>
    <tr><td class="auto-style1">Password:          </td><td> <input name="password" 
    type="password" value="" /></td></tr>
    <tr><td class="auto-style1">Re-enter Password: </td><td> <input name="password2" 
    type="password" value="" /></td></tr>
    <tr><td class="auto-style1">Phone:             </td><td> <input name="phone" 
    type="text"     value="<?php echo $phone; ?>" /></td></tr>
    <tr><td><input name="btnRegister" type="button" value="Register" onclick=
    "test_it(this.form);"/></td></tr>
    <input name="posted" type="hidden" value="">
</form>
</table>

</body>

</html>

```

```
<html>
<head>
    <title>Project Login</title>
</head>
 <script type="text/javascript" >
function test_it(f)
{
    //alert("Test");
    if (f.u_id.value == ""   || f.u_pwd.value == "")
    {
       alert("You have to enter a user ID and password!");
       return;
    }

    //changes to catch XSS and SQL injection
    if ((f.u_id.value.indexOf("<") != -1) || (f.u_pwd.value.indexOf("<") != -1) ||
    (f.u_id.value.indexOf("'") != -1) || (f.u_pwd.value.indexOf("'") != -1))
    {
       alert("You have illegal characters in user ID or password!");
       return;
    }

   //alert(f.u_id.value + ' ' + f.u_pwd.value ) ;
   f.submit();

}

</script>

<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="white">
    <table cellspacing="0" cellpadding="0" border="0" width="500" align="center">
        <tr>
            <td width="300">
                <br /><br /><br /><br />
                <form action = "cPanelLogin.php" method = "POST" name="login" id="login">
                <table cellspacing="1" cellpadding="3" style="border:1px #000000 solid" bgcolor="#BDBDBD" align="center">
                    <tr>
                        <td width="300" colspan="2">
                            <center><h1>Project Login</h1></center>
                        </td>
                    </tr>

                    <tr>
                        <td width="75">
                            Login:
                        </td>
                        <td width="225">
                            <input type="text" name="u_id" size="30">
                        </td>
                    </tr>

                    <tr>
                        <td width="75">
                            Password:
                        </td>
                        <td width="225">
                            <input type="password" name="u_pwd" size="30">
                        </td>
                    </tr>

                </table>
                <table align="center">
                    <tr>
                        <td>
                            <input type = "button" value = "Login" onclick="test_it(this.form);">
                            <input type="reset" value="Reset">
                        </td>
                    </tr>
                </table>
                </form><br>
                <table cellspacing="0" cellpadding="0" align="center">
                    <tr>
                        <td>
                            Kevin Miller & Matt Haight<br>
                            Final Project<br>
                            CMPT-483 Database Systems<br>
                            Professor Katherine G. Herbert, Ph.D.<br>
                            Montclair State University<br>
                            Fall 2012
                        </td>
                    </tr>
                </table>

            </td>
        </tr>
    </table>

</body>
</html>

```

```
<?php
//connect to database
require "mySQL.php";

if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    echo '<script type="text/javascript"> alert("You must login.");';
    echo 'window.location.replace("index.php"); </script>';
    exit();
}
?>
<html>
<head>
    <title>Taste It Again - Information</title>
    <?php //include("head.php"); ?>
</head>

<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">

    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="#82FA58">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td>
<!------------ Start of added content ---------------------------------------------------------------------------------------->

                            <center><h1>Information Coming Soon!</h1><center>
                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>
</html>

```

```php
<?php
//connect to database
require "mySQL.php";

if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    echo '<script type="text/javascript"> alert("You must login.");';
    echo 'window.location.replace("index.php"); </script>';
    exit();
}
//category filter from main menu
//$cat = $_GET['cat']; //bugfix 2012-12-16 KSM
if(isset($_GET['cat']))
    $cat = $_GET['cat'];
else
    $cat = $_POST['cat'];



$sql = "select * from PRODUCTS".((intval($cat) > 0) ? " where CATID = '$cat'" : "")." order by CATID";
//echo $sql."<br />";
if (!($menuResults = $mysqli->query($sql))){
    die("Error - cannot get menu.\n$sql");
}

//get current list of all categories - created in header.php
$userCatList = $_SESSION['userCatList'];

//get, or create cart
//unset($_SESSION['cart']); //for debugging
if (isset($_SESSION['cart'])){
    $cart = $_SESSION['cart'];
}else{
    //echo"new cart!<br />";
    $cart = array();
}

/*
//debug messages
echo "<pre>";
echo "session cart: <br />";
print_r($cart);
echo "</pre>";
*/

/*
//debug messages
echo "<pre>";
echo "POST: <br/>";
```

```
print_r($_POST);
echo "</pre>";
*/

/*
//debug messages
echo "<pre>";
echo "GET: <br/>";
print_r($_GET   );
echo "</pre>";
*/

//update cart
foreach($_POST as $key => $value){
    $arr = explode("-",$key);
    if($arr[0] == "key"){
        //if qty = 0, delete from cart; otherwise add/update
        if($value == 0){
            unset($cart[$arr[1]]);
        }
        else{
            $cart[$arr[1]] = $value;
        }
    }
}
//put updated cart back into session
$_SESSION['cart'] = $cart;

/*
//debug messages
echo "<pre>";
echo "SESSION: <br />";
print_r($_SESSION);
echo "</pre>";
*/

/*
//debug messages
echo "<pre>";
echo "updated cart: <br />";
print_r($cart);
echo "</pre>";
*/

if(isset($cart)){
    if(count($cart)==0)
        $cartStatusMsg = "You have 0 items in cart";
    else{
        $itemCount = 0;
        foreach($cart as $key => $value)
            $itemCount += $value;

        $cartStatusMsg = "You have $itemCount items in your cart.";
    }
}
?>

<script type="text/javascript" >
function validate(f){
    if(f.checkValidity()){
        f.submit();
    }else{
        alert("Invalid data - Please check all fields");
        return;
    }
}
</script>

<script type="text/javascript" >
//function viewCart(f){
//  alert("viewing cart");
//  f.action="viewcart.php";
//  alert (f.action);
//  f.submit();
//}
</script>

<html>
<head>
    <?php
        if (isset($_POST['btnViewCart'])){
            //if "View Cart" button was pressed and cart is not empty, redirect to viewcart.php after updating cart
            echo '<meta HTTP-EQUIV="REFRESH" content="0; url=viewcart.php">'."\n";
        }
    ?>
    <title>Taste It Again - Menu</title>
</head>
<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">

    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="#82FA58">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td>
<!-- CONTENT -->
                            <form name="menu" action="<?php echo $_SERVER['SCRIPT_NAME'];?>" id="menu" method = "POST">
                            <table cellspacing="0" cellpadding="0" width="900" border="0">
```

```php
<?php
    if($cartStatusMsg != ""){
        echo "<tr><td>$cartStatusMsg</td></tr>\n";
    }
?>
<tr>
    <td>
        <center><h1>Menu</h1><center>
    </td>
</tr>
<?php
    $currentCatID =0;
    $bgColor = 'white';
    if($product = $menuResults->fetch_assoc()){ //there is at least one record
        while (true){ //break when no more records
            $currentCatID = intval($product['CATID']);
            $currentCatName = $userCatList[$currentCatID];

            //output new category header
            echo "<tr>"."\n";
            echo "  <td>"."\n";
            echo "      <h2>$currentCatName</h2>\n";
            echo "  </td>"."\n";
            echo "</tr>"."\n";

            //alternate background colors
            if ($bgColor != '#BDBDBD'){
                $bgColor = '#BDBDBD';
            }else{
                $bgColor = 'white';
            }

            //print category header
            echo '<tr>'."\n";
            echo '  <td>'."\n";
            echo '      <table cellspacing="1" cellpadding="1" style="border:1px #000000 solid" bgcolor="'.$bgColor.'" align="center" width="800">'."\n";
            echo'           <tr>'."\n";
            echo'               <td width="150">'."\n";
            echo'<b><h3>Product</h3></b>'."\n";
            echo'               </td>'."\n";
            echo'               <td width="75">'."\n";
            echo'<center><b><h3>Price</h3></b></center>'."\n";
            echo'               </td>'."\n";
            echo'               <td width="150">'."\n";
            echo'<center><b><h3>Quantity</h3></b></center>'.
```

```
"\n";
echo'               </td>'."\n";
echo'           </tr>'."\n";

while (true){//break when caetgory changes or no more records
    //print record
    echo'<tr>'."\n";
    echo'   <td>'."\n";
    echo'<span title="'.$product['DESCRIPTION'].'">'."\n";
    echo'<b>'.$product['NAME'].'</b>'."\n";
    echo'   </td>'."\n";
    echo'   <td>'."\n";
    echo'       <center>$'.number_format($product['PRICE'],2).'</center>'."\n";
    echo'   </td>'."\n";
    echo'   <td>'."\n";
    $pKey = 'key-'.$product['PRODID'];
    $pQty = intval($cart[$product['PRODID']]);
    echo'       <center>
                <input type="text"
                name="'.$pKey.'"
                size="2"
                value="'.$pQty.'">
                </center>'."\n";
    echo'   </td>'."\n";
    echo'</tr>'."\n";

    //get next record
    if (!($product = $menuResults->fetch_assoc())){
        //no more records
        break;
    }

    //check if caategory changes
    if (intval($product["CATID"]) != $currentCatID){
        break;
    }//end if
} //end while same category

//print end of category table
echo'       </table>'."\n";
echo'   </td>'."\n";
echo' </tr>'."\n";

if (!($product)){
    //no more records
    break;
}
```

```
                                        }//end while records exist
                                    }//end if get record
                                ?>
                            </table>
                            <table align="center">
                                <tr>
                                    <td>
                                        <?php
                                        if((count($cart) == 0)){//cart is empty
                                            echo'<input type="submit" name="btnCreateOrder" value="Create Order">'."\n";
                                        }else{
                                            echo'<input type="submit" name="btnUpdateOrder" value="Update Order">'."\n";
                                            echo'<input type="submit" name="btnViewCart" value="View Cart" >'."\n";
                                        }
                                        ?>
                                        <input type="hidden" name="cat" value="<?php echo $cat; ?>">
                                    </td>
                                </tr>
                            </table>
                            </form>
                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr bgcolor="#82FA58">
            <td colspan="2">
                &nbsp;
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>
</html>

```

```
<?php
//connect to database
require "mySQL.php";

if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    echo '<script type="text/javascript"> alert("You must login.");';
    echo 'window.location.replace("index.php"); </script>';
    exit();
}
?>
<html>
<head>
    <title>Taste It Again - Merchandise</title>
    <?php //include("head.php"); ?>
</head>

<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">

    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="#82FA58">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td>
<!-- CONTENT -->
                            <center><h1>Merchandise</h1><center>
                        </td>
                    </tr>
                    <tr>
                        <td align="center" valign="center">
                            <h1>Coming Soon!</h1>
                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
```

```
</body>
</html>

```

```php
<?php
//connect to database and table
$db_host = 'localhost';
$db_user = 'cmpt483a_root';
$db_pwd = '&6Kmz[FOfuH$';
$database = 'cmpt483a_tasteitagain';
$mysqli = new mysqli($db_host, $db_user, $db_pwd, $database);
if ($mysqli->connect_error) {
    die('Connect Error (' . $mysqli->connect_errno . ') '
            . $mysqli->connect_error);
}

?>
```

```
<?php
//connect to database
require "mySQL.php";

if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    echo '<script type="text/javascript">'."\n";
    echo 'alert("You must login.");'."\n";
    echo 'window.location.replace("index.php");'."\n";
    echo '</script>'."\n";
    exit();
}
/*
echo "firstname  ".$_SESSION['firstname']."  <br/>";
echo "isAdmin    ".$_SESSION['isAdmin']."    <br/>";
echo "isOwner    ".$_SESSION['isOwner']."    <br/>";
echo "isCustomer ".$_SESSION['isCustomer']." <br/>";
echo "email      ".$_SESSION['email']."      <br/>";
*/

if($_SESSION['isAdmin'] != 'Y'){
    echo '<script type="text/javascript">'."\n";
    echo 'alert("Only administrators can use this page");'."\n";
    echo 'window.history.back();'."\n";
    echo '</script>'."\n";
    exit();
}

?>

<script type="text/javascript" >
function validate(f){
    if(f.checkValidity()){
        f.submit();
    }else{
        alert("Invalid data - Please check all fields");
        return;
    }
}
</script>

<html>
<head>
        <title>Taste it again - Product Admin</title>
</head>
<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">
    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="#82FA58">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td><center>
<!-- Start -------------------------------------------------------------------------------------------------------->
<?php

/*
echo "<pre>\n";
print_r($_POST);
echo "</pre>\n";
*/

//operation variables are the operation being performed by admin
$operation    = $_POST['operation'];     //SQL Operation UPDATE, INSERT, or DELETE
if ($_POST[updateFlag] == "UPDATE")
    $operation = "UPDATE";

//user-input fields for new record
$pProdID  = $_POST['pProdID'];
$pCatID   = $_POST['pCatID'];
$pCatName = $_POST['pCatName'];
$pName    = $_POST['pName'];
$pDesc    = $_POST['pDesc'];
$pPrice   = $_POST['pPrice'];
$pTax     = (strtoupper($_POST['pTax']== "Y")) ? "1" : "0";
//$pCstart  = !(strtotime($_POST['pCstart'])) ? "NULL" : $_POST['pCstart'];
//$pCend    = !(strtotime($_POST['pCend'])) ? "NULL" : $_POST['pCend'];
$pHide    = (strtoupper($_POST['pHide']== "Y")) ? "1" : "0";

//filter products table
$filterCatID = $_POST['filterCatID'];

//default values when user selected Edit
$edProdID  = $_POST['edProdID'];
$edName    = $_POST['edName'];
$edDesc    = $_POST['edDesc'];
$edCatID   = $_POST['edCatID'];
$edCatName = $_POST['edCatName'];
$edPrice   = $_POST['edPrice'];
$edTax     = ($_POST['edTax'] == "1") ? "Y" : "N";
//$edCstart  = (($_POST['edCstart'] == '0000-00-00') ? "" : $_POST['edCstart']);
//$edCend    = (($_POST['edCend']   == '0000-00-00') ? "" : $_POST['edCend']);
$edHide    = ($_POST['edHide'] == "1") ? "Y" : "N";

//buttons from each row
$btnEditProduct   = $_POST['btnEditProduct'];
$btnDeleteProduct = $_POST['btnDeleteProduct'];
```

```php
if($btnDeleteProduct == "Delete")
    $operation = "DELETE";

$posted       = $_POST['posted'];       //user submitted a form
$table        = "PRODUCTS";

//echo"operation    $operation   <br />\n";
//echo"keyFieldData $keyFieldData<br />\n";
//echo"keyFieldName $keyFieldName<br />\n";
//echo"fieldData    $fieldData   <br />\n";
//echo"fieldName    $fieldName   <br />\n";
//echo"table        $table       <br />\n";

//get list of categories
if (!($catList = $mysqli->query("select CATID, NAME from CATEGORIES;"))){
    die("Cannot get category list");
}

/*echo "posted: $posted<br />";
echo "operation: $operation<br />";
echo "keyFieldName: $keyFieldName<br />";
echo "keyFieldData: $keyFieldData<br />";
*/

//perform user selected operation
if ($posted == "Y"){
    if (($operation == "UPDATE")  && ($pProdID != ""))
    {
        /*$sql="UPDATE {$table} SET NAME            = '{$pName}',
                                  DESCRIPTION     = '{$pDesc}',
                                  CATID           = '{$pCatID}',
                                  PRICE           = '{$pPrice}',
                                  TAXABLE         = '{$pTax}',
                                  COUPONSTARTDATE = '{$pCstart}',
                                  COUPONENDDATE   = '{$pCend}',
                                  HIDEFLAG        = '{$pHide}'
                                  WHERE PRODID = '{$pProdID}';";*/

        $sql="UPDATE {$table} SET NAME            = '{$pName}',
                                  DESCRIPTION     = '{$pDesc}',
                                  CATID           = '{$pCatID}',
                                  PRICE           = '{$pPrice}',
                                  TAXABLE         = '{$pTax}',
                                  HIDEFLAG        = '{$pHide}'
                                  WHERE PRODID = '{$pProdID}';";
    }else{
        if (($operation == "DELETE") && ($edProdID != ""))
        {
            $sql="DELETE FROM {$table} WHERE PRODID = '{$edProdID}';";
            //delete $ed*
            unset($edProdID, $edName, $edDesc, $edCatID, $edCatName, $edPrice, $edTax,
            $edCstart, $edCend, $edHide);
        }else{
            if ($operation == "INSERT")
            {
//              $sql="INSERT INTO {$table} (NAME, DESCRIPTION, CATID, PRICE, TAXABLE, COUPONSTARTDATE, COUPONENDDATE, HIDEFLAG)
//                                  VALUES ('$pName', '$pDesc', '$pCatID', '$pPrice', '$pTax', '$pCstart', '$pCend', '$pHide');" ;

                $sql="INSERT INTO {$table} (NAME    , DESCRIPTION, CATID    , PRICE    , TAXABLE, HIDEFLAG)
                                    VALUES ('$pName', '$pDesc'   , '$pCatID', '$pPrice', '$pTax', '$pHide');" ;
            }else{
                if($btnEditProduct == "Edit"){ //user selected edit - no operation
                    //if user is editing existing product, get it's CATID
                    $pCatID = $edCatID;
                }else
                    echo "Error - Operation or values are incorrect. <br />";
            }
        }
    }
}

if ($sql != "")
{
    //echo "<br>attempting to run query $sql" . "<br>";
    if (!($results = $mysqli->query($sql))){
        echo("Operation query failed.<br />");
        echo("sql: $sql<br />");
    }
}


//disply edit/input table
echo "<h1>Edit Table: {$table}</h1>"."\n";
echo '<table style="border:1px #000000 solid">'."\n";
    echo '<tr>'."\n";
        echo '<td>Category</td>'."\n";
        echo '<td>Name</td>'."\n";
        echo '<td>Description</td>'."\n";
        echo '<td>Price</td>'."\n";
        echo '<td>Taxable</td>'."\n";
//      echo '<td>CpnStart</td>'."\n";
//      echo '<td>CpnEnd</td>'."\n";
        echo '<td>Hide</td>'."\n";
    echo '</tr>'."\n";
    echo '<tr>'."\n";
        echo '<td>
                <select name="pCatID" form="newProductForm" >'."\n";
                    while($row = $catList->fetch_row()){
                        echo '<option ';
                        if ($row[0] == $edCatID)
                            echo 'selected="selected" ';
                        echo 'value="'.$row[0].'">'.$row[1].'</option>'."\n";
                    }
        echo '  </select>
            </td>'."\n";

        echo '<form  name="addProduct" action="'.$_SERVER['SCRIPT_NAME'].'" method="POST"  id="newProductForm">';
        echo '<td>
                <input type="text"
                name="pName"
                required
                title="the name of the product"
                maxlength="32"
                size="10"
                value = "'.$edName.'">
            </td>'."\n";
        echo '<td>
                <input type="text"
                name="pDesc"
                title="the description of the product"
                maxlength="256"
                size="32"
                value = "'.$edDesc.'">
            </td>'."\n";
        echo '<td>
                <input type="number"
                name="pPrice"
                title="price in dollars and cents"
                pattern = "^-?\d+(\.\d{2})?$"
                maxlength="7"
                size="7"
                value = "'.$edPrice,'">
            </td>'."\n";
        echo '<td>
                <input type="text"
                name="pTax"
                title="is product taxable? Y/N"
                pattern="Y|N|y|n"
                maxlength="1"
                size="1"
                value = "'.$edTax.'">
            </td>'."\n";
/*      echo '<td>
                <input type="date"
                name="pCstart"
                title="coupon start date in yyyy-mm-dd"
                pattern="^(19|20)\d\d-(0[1-9]|1[012])-(0[1-9]|[12][0-9]|3[01])$"
                maxlength="10"
                size="10"
                value = "'.$edCstart.'">
            </td>'."\n";
        echo '<td>
                <input type="date"
                name="pCend"
                title="coupon end date in yyyy-mm-dd"
                pattern="^(19|20)\d\d-(0[1-9]|1[012])-(0[1-9]|[12][0-9]|3[01])$"
                maxlength="10"
                size="10"
                value = "'.$edCend.'">
            </td>'."\n";*/
        echo '<td>
                <input type="text"
                name="pHide"
                title="should product be hidden from menu? Y/N"
                pattern="Y|N|y|n"
                maxlength="1"
                size="1";
                value = "'.$edHide.'">
            </td>'."\n";
    echo '</tr>'."\n";
    echo "\n".'<input type="hidden" name="posted"      value="Y">';
    echo "\n".'<input type="hidden" name="pProdID"     value="'.$edProdID.'">';
    echo "\n".'<input type="hidden" name="filterCatID" value="'.$filterCatID.'">';
    if ($btnEditProduct == "Edit"){
        echo "\n".'<tr><td colspan = "8" align="center"><input type="button" value="Update" onclick="validate(this.form)" >';
        echo "\n".'<input type="hidden" name="operation"     value="UPDATE">';
    }else{
        echo "\n".'<tr><td colspan = "8" align="center"><input type="button" value="Add Product" onclick="validate(this.form)" >';
        echo "\n".'<input type="hidden" name="operation"     value="INSERT">';
    }
    echo "\n".'</form>';
echo "\n".'</table><br /><br />';

// Get all table (or filtered) data
//echo "filterCatID: ".$filterCatID."<br />\n";
if(intval($filterCatID) > 0){
    $sql = "SELECT p.* , c.NAME AS 'CATNAME'
    FROM PRODUCTS p
    LEFT JOIN CATEGORIES c ON p.CATID = c.CATID
    WHERE p.CATID = '".$filterCatID."'
    ORDER BY CATNAME";
}else{
    $sql = "SELECT p.* , c.NAME AS 'CATNAME'
    FROM PRODUCTS p
    LEFT JOIN CATEGORIES c ON p.CATID = c.CATID
    ORDER BY CATNAME";
}
//echo $sql;
if (!($results = $mysqli->query($sql))){
    die("Query to show fields from table failed: $sql");
}

echo '<table><tr><td>';
echo '<select name="filterCatID" form="filterForm" >'."\n";
            echo '<option value="none">None</option>';
```

```php
            $catList->data_seek(0);
            while($row = $catList->fetch_row()){
                echo '<option ';
                if ($row[0] == $filterCatID)
                    echo 'selected="selected" ';
                echo 'value="'.$row[0].'">'.$row[1].'</option>'."\n";
            }
echo '  </select>'."\n";
echo '</td><td>';
echo '<form  name="filter" action="'.$_SERVER['SCRIPT_NAME'].'"  method="POST" id="filterForm">'."\n";
echo '<input type="submit" name="btnFilter" value="Filter">'."\n";
echo '</form>'."\n";
echo '</td></tr></table>';

echo '<table style="border:1px #000000 solid" bgcolor="white">';
//$finfo = $results->fetch_fields();
//foreach ($finfo as $val) {
//  echo "<td>{$val->name}</td>";}

echo "<tr>\n";
echo '<td>PRODID</td>'."\n";
echo '<td>NAME</td>'."\n";
echo '<td>CATNAME</td>'."\n";
echo '<td>PRICE</td>'."\n";
echo '<td>TAXABLE</td>'."\n";
//echo '<td>Cpn Start</td>'."\n";
//echo '<td>CpnEnd</td>'."\n";
echo '<td>HIDEFLAG</td>'."\n";
echo "</tr>\n";

// printing table rows
while($row = $results->fetch_assoc())
{
    echo "<tr>";
    echo "<tr>\n";
    echo '<td>'.$row['PRODID']     .'</td>'."\n";
    echo '<td><span title="'.$row['DESCRIPTION'].'"><b>'.$row['NAME'].'</b></span></td>'."\n";
    echo '<td>'.$row['CATNAME']    .'</td>'."\n";
    echo '<td>'.number_format($row['PRICE'],2).'</td>'."\n";
    echo '<td>'.(($row['TAXABLE'] == "1") ? "Y" : "N").'</td>'."\n";
//  echo '<td>'.(($row['COUPONSTARTDATE'] == '0000-00-00') ? "" : $row['COUPONSTARTDATE']).'</td>'."\n";
//  echo '<td>'.(($row['COUPONENDDATE'] == '0000-00-00')   ? "" : $row['COUPONENDDATE'])  .'</td>'."\n";
    echo '<td>'.(($row['HIDEFLAG'] == "1") ? "Y" : "N").'</td>'."\n";
    echo '<form action="'.$_SERVER['SCRIPT_NAME'].'" method="POST">'."\n";
    echo '<td><input type="submit" name="btnEditProduct" value="Edit"                              ></td>'."\n";
    echo '<td><input type="submit" name="btnDeleteProduct" value="Delete"                            ></td>'."\n";
    echo '    <input type="hidden" name="filterCatID"      value="'.$filterCatID.
    '"                  >'."\n";
    echo '    <input type="hidden" name="posted"
    value="Y"                                 >'."\n";//
    echo '    <input type="hidden" name="edProdID"         value="'.$row['PRODID'].
    '"                >'."\n";//
    echo '    <input type="hidden" name="edName"           value="'.$row['NAME'].
    '"                  >'."\n";//
    echo '    <input type="hidden" name="edDesc"           value="'.$row['DESCRIPTION'].
    '"           >'."\n";//
    echo '    <input type="hidden" name="edCatID"          value="'.$row['CATID'].
    '"                 >'."\n";//
    echo '    <input type="hidden" name="edPrice"          value="'.number_format($row[
    'PRICE'],2).'">'."\n";//
    echo '    <input type="hidden" name="edTax"            value="'.$row['TAXABLE'].
    '"               >'."\n";//
//  echo '    <input type="hidden" name="edCstart"
value="'.$row['COUPONSTARTDATE'].'"       >'."\n";//
//  echo '    <input type="hidden" name="edCend"
value="'.$row['COUPONENDDATE'].'"         >'."\n";//
    echo '    <input type="hidden" name="edHide"           value="'.$row['HIDEFLAG'].
    '"              >'."\n";//
    echo '    <input type="hidden" name="edCatName"        value="'.$row['CATNAME'].
    '"               >'."\n";//
    echo "</form>";
    echo "</tr>\n";
}
echo "</table>";

$results->close();
?>


<!-- End
-----------------------------------------------------------------------------------------
----------------->
                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>

</html>
```

```
<?php
if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    //they have not tried to login, or logged out
    echo '<script type="text/javascript"> alert("You must login first");';
    echo 'window.location.replace("index.php"); </script>';
    exit();
}
?>

<html>
<head>
    <title>Taste It Again - Register</title>
</head>
<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">
<script type="text/javascript">
<!--
function test_it(f){
    if((f.fName.value == '') ||
        (f.lName.value == '') ||
        (f.address.value == '') ||
        (f.city.value == '') ||
        (f.state.value == '') ||
        (f.zipCode.value == '') ||
        (f.email.value == '') ||
        (f.password.value == '') ||
        (f.password2.value == '') ||
        (f.phone.value == '')){
            alert("All fields must be completed.");
            return;
        }

        if(f.password.value != f.password2.value){
            alert("Passwords do not match.");
            return;
        }

        f.posted.value = "OK";
        f.submit();
}
//-->
</script>

<?php
require "mySQL.php";

/*
//debug messages
echo '<pre>';
echo "post<br />";
print_r($_POST);
echo '</pre>';
*/

$fName    = $_POST['fName'];
$lName    = $_POST['lName'];
$address  = $_POST['address'];
$address2 = $_POST['address2'];
$city     = $_POST['city'];
$state    = $_POST['state'];
$zipCode  = $_POST['zipCode'];
$email    = $_POST['email'];
$password = $_POST['password'];
$phone    = $_POST['phone'];
$txtflag  = ($_POST['txtflag'] == "1") ? "1":"0";
$mailflag = ($_POST['mailflag'] == "1") ? "1":"0";
$posted   = $_POST['posted'];
$hash     = md5($password);

if ($posted == "OK"){
    $sql1 = "insert into USERS (EMAILADD,  PWHASH, FIRSTNAME, LASTNAME,   PHONE, CUSTFLAG)
                         VALUES('$email', '$hash',  '$fName', '$lName','$phone', 'Y');";

    $sql2 = "select USERID from USERS where EMAILADD = '$email';";

    //transaction begin with implicit autocommit off
    //echo "starting transaction<br />";
    if (!$mysqli->query("START TRANSACTION;")){
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Start transaction failed: '.$mysqli->error.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }

    //insert into USERS table
    //echo "inserting to USERS<br />";
    //echo $sql1."<br />";
    if (!$mysqli->query($sql1)){
        //rollback
        $err = $mysqli->error; //save error message before rollback
        $mysqli->query("ROLLBACK;"); //must add check for rollback failure
        echo "sql1: $sql1<br />\n";
        echo "err: $err<br />\n";
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Account creation failed: '.$err.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }

```

```php
    //retrieve auto-increment USERID
    //echo "getting userid<br />";
    //echo $sql2."<br />";
    if (!($result = $mysqli->query($sql2))){
        //rollback
        $err = $mysqli->error; //save error message before rollback
        $mysqli->query("ROLLBACK;"); //must add check for rollback failure
        echo $sql2."<br />";
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Account creation failed: '.$err.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }

    //echo"<pre>";
    //  print_r($result);
    //echo"</pre>";

    $row = $result->fetch_assoc();
    $userid = $row['USERID'];
    //echo "userid: $userid <br />";
    $sql3 = "insert into CUSTOMERS ( USERID,  ADDLINE1,     ADDLINE2,    CITY,
    STATE,        ZIP,   EMAILFLAG, TXTMSGFLAG)
                             VALUES($userid, '$address', '$address2', '$city', '$state
                             ', '$zipCode', '$mailflag', '$txtflag');";
    //echo $sql3."<br />";

    //insert customer information
    //echo "inserting CUSTOMER<br />";
    //echo $sql3."<br />";
    if (!$mysqli->query($sql3)){
        $err = $mysqli->error; //save error message before rollback
        //rollback
        $mysqli->query("ROLLBACK;"); //must add check for rollback failure
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Account creation failed: '.$err.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }
    //commit transaction
    //echo "commting<br />";
    if ($mysqli->query("COMMIT;")){
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Account created");'."\n";
        echo '</script>'."\n";
        $_SESSION['isCustomer'] = "Y";
    }else{
        echo '<script type="text/javascript">'."\n";
        echo 'alert("Commit transaction failed: '.$mysqli->error.'");'."\n";
        echo 'window.back();';
        echo '</script>'."\n";
        exit();
    }

}
?>

    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="#82FA58">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td>
<!------------ Start of main content ---------------------------------------------------------------------------------------->
                            <table cellspacing="0" cellpadding="0" width="900" border="0">
                                <tr>
                                    <td>
                                        <center><h1>Register</h1></center>
                                    </td>
                                </tr>
                            </table>
                            <form name="register" id="register" action = '' method = "post">
                            <table cellspacing="1" cellpadding="3" style="border:1px #000000 solid" bgcolor="#BDBDBD" align="center">
                                <tr>
                                    <td>
                                        First Name
                                    </td>
                                    <td>
                                        <input type="text" name="fName" size="20" value="<?php echo $fName; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Last Name
                                    </td>
                                    <td>
                                        <input type="text" name="lName" size="20" value="<?php echo $lName; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Address
                                    </td>
                                    <td>
                                        <input type="text" name="address" size="20" value="<?php echo $address; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Address Line 2
                                    </td>
                                    <td>
                                        <input type="text" name="address2" size="20" value="<?php echo $address2; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        City
                                    </td>
                                    <td>
                                        <input type="text" name="city" size="20" value="<?php echo $city; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        State
                                        <input type="text" name="state" size="3" value="<?php echo $state; ?>">
                                    </td>
                                    <td>
                                        Zip Code
                                        <input type="text" name="zipCode" size="5" value="<?php echo $zipCode; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Phone Number
                                    </td>
                                    <td>
                                        <input type="text" name="phone" size="20" value="<?php echo $phone; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Email Address
                                    </td>
                                    <td>
                                        <input type="text" name="email" size="30" value="<?php echo $email; ?>">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Password
                                    </td>
                                    <td>
                                        <input type="password" name="password" size="20" value="" >
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Re-Enter Password
                                    </td>
                                    <td>
                                        <input type="password" name="password2" size="20" value="">
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Send me email coupons
                                    </td>
                                    <td>
                                        <input type="radio" name="mailflag" value="1" <?php echo ($mailflag == "1")?"checked":""; ?> >Y
                                        <input type="radio" name="mailflag" value="0" <?php echo ($mailflag == "0")?"checked":""; ?> >N
                                    </td>
                                </tr>
                                <tr>
                                    <td>
                                        Send me txt message coupons
                                    </td>
                                    <td>
                                        <input type="radio" name="txtflag" value="1" <?php echo ($txtflag == "1")?"checked":""; ?> >Y
                                        <input type="radio" name="txtflag" value="0" <?php echo ($txtflag == "0")?"checked":""; ?> >N
                                    </td>
                                </tr>
                            </table>
                            <table align="center">
                                <tr>
                                    <td>
                                        <input name="btnRegister" type="button" value="Register" onclick="test_it(this.form);"/>
                                        <input type="reset" value="Reset">
                                    </td>
                                </tr>
                            </table>
                            <input name="posted" type="hidden" value="">
                            </form>
                        </td>
```

```
                    </tr>
                </table>
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>
</html>

```

```php
<?php
//connect to database
require "mySQL.php";

if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    echo '<script type="text/javascript"> alert("You must login.");';
    echo 'window.location.replace("index.php"); </script>';
    exit();
}

/*
//debug messages
echo "<pre>";
echo "SESSION: <br />";
print_r($_SESSION);
echo "</pre>";
*/

$cart = $_SESSION['cart'];
/*
//debug messages
echo "<pre>";
echo "session cart: <br />";
print_r($cart);
echo "</pre>";
*/

//check if cart exists or is empty
//check cart before re-directing
if (count($cart) == 0){
    echo '<script type="text/javascript"> ';
    echo 'alert("Your cart is empty.");';
    echo '</script>';
}

//get all products where $cart[key] = PRODID
$plist = "";
foreach($cart as $key => $value){
    $plist = $plist."'".$key."', ";
}
//remove last comma
$plist = substr($plist,0,strlen($plist)-2);
$sql = "select * from PRODUCTS where PRODID in (".$plist.") order by CATID";
//echo $sql."<br />";
if (!($menuResults = $mysqli->query($sql))){
    die("Error - cannot get menu.\n$sql");
}

//get current list of all categories - created in header.php
```

```
$userCatList = $_SESSION['userCatList'];

/*
//debug messages
echo "<pre>";
echo "POST: <br/>";
print_r($_POST);
echo "</pre>";
*/

//update cart
foreach($_POST as $key => $value){
    $arr = explode("-",$key);
    if($arr[0] == "key"){
        //if qty = 0, delete from cart; otherwise add/update
        if($value == 0){
            unset($cart[$arr[1]]);
        }else
            $cart[$arr[1]] = $value;
    }
}
$_SESSION['cart'] = $cart;

/*
//debug messages
echo "<pre>";
echo "updated cart: <br />";
print_r($cart);
echo "</pre>";
*/

//check which, if any buttons were clicked
//$btnCreateUpdate = $_POST['btnCreateUpdate'];
//$btnCheckOut = $_POST['btnCheckOut'];


if(count($cart)==0)
    $cartStatusMsg = "Order NOT created - you have 0 items in cart";
else{
    $itemCount = 0;
    foreach($cart as $key => $value){
        $itemCount += $value;
    }

    $cartStatusMsg = "You have $itemCount items in your cart.";
}
?>

<script type="text/javascript" >
function validate(f){
    if(f.checkValidity()){
        f.submit();
    }else{
        alert("Invalid data - Please check all fields");
        return;
    }
}
</script>

<script type="text/javascript" >
function viewCart(f){
    alert("viewing cart");
    f.action="viewcart.php";
    alert (f.action);
    f.submit();
}
</script>

<html>
<head>
    <?php
        if (isset($_POST['btnCheckOut'])){
            if($_SESSION['isCustomer'] != 'Y'){
                echo '<script type="text/javascript"> ';
                echo 'alert("You must login or create an account before you can checkout.");';
                echo '</script>';
            }else{
                //if "Check Out" button was pressed and cart is not empty, redirect to checkout.php after updating cart
                echo '<meta HTTP-EQUIV="REFRESH" content="0; url=checkout.php">'."\n";
            }
        }
    ?>

    <title>Taste It Again - View Order</title>
</head>
<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">
    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="#82FA58">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td>
                            <form name="menu" action="<?php echo $_SERVER['SCRIPT_NAME'];?>" id="menu" method = "POST">
                            <table cellspacing="0" cellpadding="0" width="900" border="0">
                                <tr>
                                <?php
                                    echo "<tr><td>$cartStatusMsg</td></tr>\n";
```

```
?>
    <td>
        <center><h1>ORDER</h1><center>
    </td>
</tr>
<?php
    $currentCatID =0;
    $bgColor = 'white';

    //print category header
    echo '<tr>'."\n";
    echo '  <td>'."\n";
    echo '      <table cellspacing="1" cellpadding="1" style="border:1px #000000 solid" bgcolor="'.$bgColor.'" align="center" width="800">'."\n";
    echo'           <tr>'."\n";
    //echo'                 <td width="150">'."\n";
    echo'               <td>'."\n";
    echo'                   <b><h3>Category</h3></b>'."\n";
    echo'               </td>'."\n";
    //echo'                 <td width="100">'."\n";
    echo'               <td>'."\n";
    echo'                   <b><h3>Product</h3></b>'."\n";
    echo'               </td>'."\n";
    //echo'                 <td width="75">'."\n";
    echo'               <td>'."\n";
    echo'                   <center><b><h3>Price</h3></b></center>'."\n";
    echo'               </td>'."\n";
    //echo'                 <td width="150">'."\n";
    echo'               <td>'."\n";
    echo'                   <center><b><h3>Quantity</h3></b></center>'."\n";
    echo'               </td>'."\n";
    echo'               <td>'."\n";
    echo'                   <center><b><h3>Ext Price</h3></b></center>'."\n";
    echo'               </td>'."\n";
    echo'           </tr>'."\n";

    if($product = $menuResults->fetch_assoc()){ //there is at least one record
        $total = 0;
        while (true){ //break when no more records
            $currentCatID = intval($product['CATID']);
            $currentCatName = $userCatList[$currentCatID];

            //output new category header
            //echo "<tr>"."\n";
            //echo "    <td>"."\n";
```

```php
                                            //echo "        <h2>$currentCatName</h2>\n";
                                            //echo "    </td>"."\n";
                                            //echo "</tr>"."\n";

                                            //alternate background colors
                                            if ($bgColor != '#BDBDBD'){
                                                $bgColor = '#BDBDBD';
                                            }else{
                                                $bgColor = 'white';
                                            }

                                            //category header was here

                                            while (true){//break when caetgory changes or no more records
                                                //print record
                                                echo'<tr>'."\n";
                                                echo'   <td>'."\n";
                                                echo'<b>'.$currentCatName.'</b>'."\n";
                                                echo'   </td>'."\n";
                                                echo'   <td>'."\n";
                                                echo'<span title="'.$product['DESCRIPTION'].'">'."\n";
                                                echo'<b>'.$product['NAME'].'</b>'."\n";
                                                echo'   </td>'."\n";
                                                echo'   <td>'."\n";
                                                echo'       <center>$'.number_format($product['PRICE'],2).'</center>'."\n";
                                                echo'   </td>'."\n";
                                                echo'   <td>'."\n";
                                                $pKey = 'key-'.$product['PRODID'];
                                                $pQty = intval($cart[$product['PRODID']]);
                                                echo'       <center>
                                                            <input type="text"
                                                            name="'.$pKey.'"
                                                            size="2"
                                                            value="'.$pQty.'">
                                                            </center>'."\n";
                                                echo'   </td>'."\n";
                                                echo'   <td align="right">'."\n";
                                                $extprice = $pQty*$product['PRICE'];
                                                $total += $extprice;
                                                echo'$'. number_format($extprice,2);
                                                echo'   </td>'."\n";
                                                echo'</tr>'."\n";

                                                //get next record
                                                if (!($product = $menuResults->fetch_assoc())){
                                                    //no more records
                                                    break;
                                                }
```

```

                    //check if category changes
                    if (intval($product["CATID"]) != $currentCatID){
                        break;
                    }//end if
                } //end while same category

                if (!($product)){
                    //no more records
                    break;
                }
            }//end while records exist

            //print end of products table
            echo'           <tr>
                                <td></td>
                                <td></td>
                                <td></td>
                                <td align="right">Total:</td>
                                <td align="right">$'.number_format($total,2).'</td>
                            </tr>';

            echo'       </table>'."\n";
            echo'   </td>'."\n";
            echo' </tr>'."\n";

        }//end if get record
    ?>
</table>
<table align="center">
    <tr>
        <td>
            <?php
                if((count($cart) == 0)){//cart is empty
                    echo'<input type="submit" name="btnCreateOrder" value="Create Order">'."\n";
                }else{
                    echo'<input type="submit" name="btnUpdateOrder" value="Update Order">'."\n";
                    echo'<input type="submit" name="btnCheckOut" value="Check Out" >'."\n";
                }
            ?>
        </td>
    </tr>
</table>
</form>
```

```
                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr bgcolor="#82FA58">
            <td colspan="2">
                &nbsp;
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>
</html>

```

```
<?php
//connect to database
require "mySQL.php";

if (!@session_start()){
    die("Cannot start session");
}

if (!isset($_SESSION['valid_user'])){
    echo '<script type="text/javascript"> alert("You must login.");';
    echo 'window.location.replace("index.php"); </script>';
    exit();
}

if(!($_SESSION['isOwner'] == 'Y')){
    echo '<script type="text/javascript"> ';
    echo 'alert("You must logged in as owner to view orders.");';
    echo 'window.location = '."'".$_SERVER['HTTP_REFERER']."'";
    echo '</script>';
    exit();
}

$sql = "select * from ORDERS";
if(!($orders = $mysqli->query($sql))){
    die("ORDERS - could not get records.");
}
?>

<html>
<head>
    <title>Taste it Again - Home</title>
    <?php //include("head.php"); ?>
</head>

<body leftmargin="0px" topmargin="0px" marginwidth="0px" marginheight="0px" bgcolor="black">
    <table cellspacing="0" cellpadding="0" width="900" align="center" border="0">

        <?php include("header.php"); ?>

        <tr height="500" bgcolor="#82FA58">
            <td colspan="2">
                <table cellspacing="0" cellpadding="0" width="900" border="0" height="100%">
                    <tr valign="top">
                        <td>
<!------------- Start of added content ---------------------------------------------------------------------------------------->

                            <center><h1>View Orders</h1><center>
                            <table style="border:1px solid black" align="center" bgcolor="white">
                                <tr>
```

```
                                    <td>Order ID</td>
                                    <td>Name</td>
                                    <td>Phone</td>
                                    <td>Address 1</td>
                                    <td>Address 2</td>
                                    <td>City</td>
                                    <td>State</td>
                                    <td>Zip</td>
                                    <td>Time</td>
                                </tr>
                                <?php
                                    while($row = $orders->fetch_assoc()){
                                    echo '<tr>';
                                    echo '  <td><a href="displayorder.php?ordUID='.$row['ORDID'].'&calledBy=owner">'.$row['ORDID'].'</a></td>';
                                    echo '  <td>'.$row['FULLNAME'].'</td>';
                                    echo '  <td>'.$row['CONTACTPHONE'].'</td>';
                                    echo '  <td>'.$row['DELADDLINE1'].'</td>';
                                    echo '  <td>'.$row['DELADDLINE2'].'</td>';
                                    echo '  <td>'.$row['DELCITY'].'</td>';
                                    echo '  <td>'.$row['DELSTATE'].'</td>';
                                    echo '  <td>'.$row['DELZIP'].'</td>';
                                    echo '  <td>'.$row['TIME'].'</td>';
                                    echo '</tr>';
                                    }
                                ?>
                            </table>
<!------------- End of added content ----------------------------------------------------------------------------------------->

                        </td>
                    </tr>
                </table>
            </td>
        </tr>
        <tr height="30px" bgcolor="#FFFF00">
            <td colspan="2">

                <?php include("footer.php"); ?>

            </td>
        </tr>
    </table>
</body>
</html>

```