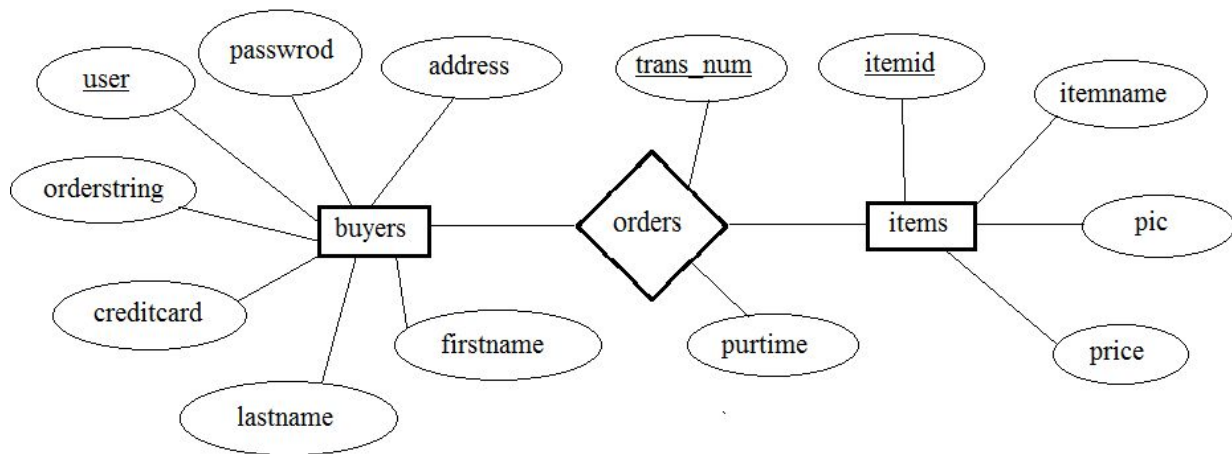


## E-Mall Final Report

E-Mall is an online shopping cart app that could be used by a small businesses to sell their products. It is hosted on FAU's lamp server and could be accessed at <http://lamp.cse.fau.edu/~mhus2015/eball/> Moreover, E-Mall app is connected to the database and is based on the ER diagram below.



In the ER diagram above, one can notice that there are two entity tables (buyers, items) and one relationship table (orders). The buyers' table consists of seven attributes such as address, password orderstring, creditcard, lastname, firstname, and user that is also a primary key. On the other hand, the items table has only four attributes like itemname, pic, price, and itemid that is a primary key. The last table is an order table that holds the relationship between buyers and items table. There are no special participation requirements in this ER diagram. Buyers are free to order as many items as they want and there are no limitation to how many orders they can make. They do not have to make any order if they do not what to.

E-Mall app was implemented with use of various languages like HTML, CSS, PHP, MySQL, and JavaScript. Additionally, software like WinSCP, Brackets, Notepad, and CyberDuck were used to create E-Mall application that is hosted on lamp server.

In php/db\_connect.php, PHP code connects with the database and defines php function that calls MySQL that will create future tables if they do not exist.

```
1  <?php
2
3  $dbhost = 'localhost'; // Most likely will not need to be changed
4  $dbname = 'mhus2015'; // Needs to be changed to your designated table database name
5  $dbuser = 'mhus2015'; // Needs to be changed to reflect your LAMP server credentials
6  $dbpass = '*****'; // Needs to be changed to reflect your LAMP server credentials
7
8
9  $connection = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
10 if ($connection->connect_error) die($connection->connect_error);
11
12 function createTable($name, $query)
13 {
14     queryMysql("CREATE TABLE IF NOT EXISTS $name($query)");
15 }
16
17
18
19 function queryMysql($query)
20 {
21     global $connection;
22     $result = $connection->query($query);
23     if (!$result) die($connection->error);
24     return $result;
25 }
```

Next, the database tables are created in the setup.php where PHP code calls MySQL queries. As shown below, three tables are created if they do not already exist in the database.

```

4  createTable ('buyers',
5      'user varchar(32) primary key unique,
6      password varchar(32),
7      firstname varchar(32),
8      lastname varchar(32),
9      address varchar(50),
0      creditcard varchar(50),
1      orderstring varchar(24)');
2
3  createTable('items',
4      'itemid int unsigned primary key unique,
5      itemname varchar(32),
6      price real,
7      pic LONGBLOB');
8
9  createTable('orders',
0      'trans_num int unsigned primary key AUTO_INCREMENT,
1      user varchar(32) NOT NULL,
2      orderstring varchar(24) ,
3      purtime timestamp,
4      FOREIGN KEY (user)
5          REFERENCES buyers(user),
6      FOREIGN KEY (orderstring)
7          REFERENCES buyers(orderstring)');
8

```

User may browse through E-Mall without being registered users. However, to make any purchases individuals need to sign up with E-Mall. Their information will be stored on lamp server in the buyers' table.

```

if ($user=="" || $pass=="" || $firstname=="" || $lastname=="" || $address=="" || $creditcard=="")
    $error = "<center>Not all fields were entered</center><br>";
else
{
    $result = queryMysql("SELECT * FROM buyers WHERE user='$user'");

    if ($result->num_rows)
        $error = "That username already exists<br><br>";
    else
    {
        $token    = hash('ripemd128', "$salt1$pass$salt2");
        $orderstring = "00000000000000000000000000000000";
        queryMysql("INSERT INTO buyers VALUES('$user', '$token', '$firstname',
        '$lastname' , '$address', '$creditcard','$orderstring')");
    }
}

```

After user registration, he will need to log in with his username and password that was stored in the database. The PHP code that calls MySQL query to check if the user and password

is in the database and if it is correct.

```
if (isset($_POST['user']))
{
    $user = sanitizeString($_POST['user']);
    $pass = sanitizeString($_POST['pass']);

    if ($user == "" || $pass == "")
        $error = "<div class='error-1'>PLEASE ENTER YOUR DETAILS TO LOG IN</div><div class='error-1'>Some Fields Are Blank</div>";
    else
    {
        $token = hash('ripemd128', "$salt1$pass$salt2");
        $result = queryMySQL("SELECT * FROM buyers WHERE user='$user' AND password='$token'");

        if ($result->num_rows == 0)
        {
            $error = "<div class='error-4'>INVALID USERNAME/PASSWORD </div>";
        }
        else
        {
            $_SESSION['user'] = $user;
            $_SESSION['pass'] = $pass;
            die(header('Location: http://lamp.cse.fau.edu/~mhus2015/email/userpage.php'));
        }
    }
}
```

When users are logged in, they may access their profile page by clicking on their name.

After doing so, userprofile.php will call MySQL functions to retrieve the users data from the database. Then, the user may modify his information that will be updated in the database and on the page.

```
68     $result = queryMySQL("SELECT * FROM buyers WHERE user='$user'");
69         if($result->num_rows != 0)
70         {
71             while($rows = $result->fetch_assoc())
72             {
73                 $cfname = $fname = $rows['firstname'];
74                 $clname = $lname = $rows['lastname'];
75                 $username = $rows['user'];
76                 $caddr = $address = $rows['address'];
77                 $cccn = $creditcard = $rows['creditcard'];
78                 $cpass = $password = $rows['password'];
79             }
80         }
```

```
$UpdateQuery = "
UPDATE buyers SET
password='$token'
WHERE user='$username'";

if($connection->query($UpdateQuery)===TRUE)
{
    echo "Password Was Updated<br><br>";
}
else
{
    echo "Error updating record: ". $connection->error;
}
}
else {$password = $cpass;}
if ($fname != "" )
{
    $UpdateQuery = "
UPDATE buyers SET
firstname='$fname'
WHERE user='$username'";

    if($connection->query($UpdateQuery)===TRUE)
    {
        echo "First Name Was Updated<br><br>";
    }
    else
    {
        echo "Error updating record: ". $connection->error;
    }
}
}
else {$fname = $cfn;}
```

```

if ($lname != "")
{
    $UpdateQuery = "
    UPDATE buyers SET
    lastname='$lname'
    WHERE user='$username'";
    if($connection->query($UpdateQuery)===TRUE)
    { echo "Last Name Was Updated<br><br>"; }
    else { echo "Error updating record: ". $connection->error; }
} else {$lname = $cln;}
if ($address != "" ) {
    $UpdateQuery = "
    UPDATE buyers SET
    address='$address'
    WHERE user='$username'";
    if($connection->query($UpdateQuery)===TRUE)
    { echo "Address Was Updated<br><br>"; }
    else { echo "Error updating record: ". $connection->error; }
} else {$address = $cadr;}
if ($creditcard != "")
{
    $UpdateQuery = "
    UPDATE buyers SET
    creditcard='$creditcard'
    WHERE user='$username'";
    if($connection->query($UpdateQuery)===TRUE)
    {echo "Credit Card Number Was Updated<br><br>"; }
    else { echo "Error updating record: ". $connection->error; }
} else {$creditcard = $cccn;}

```

Additionally, a user may delete their account if they feel like they would not need to use it or if they would like to create new one with different username.

```

<?php
    require_once 'header.php';

    $UpdateQuery = "
    DELETE From buyers
    WHERE user='$user'";

    if($connection->query($UpdateQuery)===TRUE)
    {
        if (isset($_SESSION['user'])) destroySession();
        die(header('Location: http://lamp.cse.fau.edu/~mhus2015/emall'));
    }
    else
    {
        echo "Error updating record: ". $connection->error;
    }
}
?>

```



The last part of the E-Mall application is a checkout functionality. In the checkout.php first query to be called is the one to connect the database with PHP code. Then, the user's order information in the orderstring is being updated accordingly to the user's order. Then, the orderstring is being checked for what needs to be retrieved and displayed from the database.

```
$result = queryMysql("SELECT * FROM buyers WHERE user='$user'");
if($result->num_rows !=0)
{
    while($rows = $result->fetch_assoc())
    {
        $username = $rows['user'];
        $orderstring = $rows['orderstring'];
    }
}
else{
    echo"no result";
}

if(isset($_POST['btnGCB']))
{
    $qtyGCB = $_POST['qtyGCB']; // Storing Selected Value In Variable   ///
    $temp = substr_replace($orderstring,$qtyGCB, 0 , 2 );
    $UpdateQuery = "
        UPDATE buyers SET
        orderstring='$temp'
        WHERE user='$user'";
    if($connection->query($UpdateQuery)===TRUE)
    {
        // echo "Password Was name<br><br>";
    }
}

if(isset($_POST['btnHTC']))
{
    $qtyHTC = $_POST['qtyHTC']; // Storing Selected Value In Variable   ///
    $temp = substr_replace($orderstring,$qtyHTC, 2 , 2 );
    $UpdateQuery = "
        UPDATE buyers SET
        orderstring='$temp'
        WHERE user='$user'";
    if($connection->query($UpdateQuery)===TRUE)
```

```

if(isset($_POST['btnPVR'])) {
    $qtyGCB = $_POST['qtyPVR']; // Storing Selected Value In Variable    ///
    $temp = substr_replace($orderstring,$qtyGCB, 4 , 2 );
    $UpdateQuery = "
        UPDATE buyers SET
        orderstring='$temp'
        WHERE user='$user'";
    if($connection->query($UpdateQuery)===TRUE)
    { echo "Password Was name<br><br>";    }    }

if(isset($_POST['btnOVR'])) {
    $qtyHTC = $_POST['qtyOVR']; // Storing Selected Value In Variable    ///
    $temp = substr_replace($orderstring,$qtyHTC, 6 , 2 );
    $UpdateQuery = "
        UPDATE buyers SET
        orderstring='$temp'
        WHERE user='$user'";
    if($connection->query($UpdateQuery)===TRUE)
    { echo "Password Was name<br><br>"; } }

if(isset($_POST['btnAC'])) {
    $qtyGCB = $_POST['qtyAC']; // Storing Selected Value In Variable    ///
    $temp = substr_replace($orderstring,$qtyGCB, 8 , 2 );
    $UpdateQuery = "
        UPDATE buyers SET
        orderstring='$temp'
        WHERE user='$user'";
    if($connection->query($UpdateQuery)===TRUE)
    { echo "Password Was name<br><br>"; }}

if(isset($_POST['btnAS'])) {
    $qtyHTC = $_POST['qtyAS']; // Storing Selected Value In Variable    ///
    $temp = substr_replace($orderstring,$qtyHTC, 10 , 2 );
    $UpdateQuery = "
        UPDATE buyers SET
        orderstring='$temp'
        WHERE user='$user'";
    if($connection->query($UpdateQuery)===TRUE)
    {echo "Password Was name<br><br>";}}

```



```

if(isset($_POST['btnHP'])){
    $qtyGCB = $_POST['qtyHP']; // Storing Selected Value In Variable    ///
    $temp = substr_replace($orderstring,$qtyGCB, 12 , 2 );
    $UpdateQuery = "
        UPDATE buyers SET
        orderstring='$temp'
        WHERE user='$user'";
    if($connection->query($UpdateQuery)===TRUE)
    {echo "Password Was name<br><br>";}}

if(isset($_POST['btnMB'])){
    $qtyHTC = $_POST['qtyMB']; // Storing Selected Value In Variable    ///
    $temp = substr_replace($orderstring,$qtyHTC, 14 , 2 );
    $UpdateQuery = "
        UPDATE buyers SET
        orderstring='$temp'
        WHERE user='$user'";
    if($connection->query($UpdateQuery)===TRUE)
    {echo "Password Was name<br><br>";}}

if(isset($_POST['btnVI'])){
    $qtyGCB = $_POST['qtyVI']; // Storing Selected Value In Variable    ///
    $temp = substr_replace($orderstring,$qtyGCB, 16 , 2 );
    $UpdateQuery = "
        UPDATE buyers SET
        orderstring='$temp'
        WHERE user='$user'";
    if($connection->query($UpdateQuery)===TRUE)
    { echo "Password Was name<br><br>";}}

if(isset($_POST['btnHU'])){
    $qtyHTC = $_POST['qtyHU']; // Storing Selected Value In Variable    ///
    $temp = substr_replace($orderstring,$qtyHTC, 18 , 2 );
    $UpdateQuery = "
        UPDATE buyers SET
        orderstring='$temp'
        WHERE user='$user'";
    if($connection->query($UpdateQuery)===TRUE)
    { echo "Password Was name<br><br>";}}

```

```

if(isset($_POST['btnIP']))
{ $qtyGCB = $_POST['qtyIP']; // Storing Selected Value In Variable
  $temp = substr_replace($orderstring,$qtyGCB, 20 , 2 );
  $UpdateQuery = "
    UPDATE buyers SET
    orderstring='$temp'
    WHERE user='$user'";
  if($connection->query($UpdateQuery)===TRUE)
  { echo "Password Was name<br><br>"; } }

if(isset($_POST['btnSM']))
{ $qtyHTC = $_POST['qtySM']; // Storing Selected Value In Variable
  $temp = substr_replace($orderstring,$qtyHTC, 22, 2 );
  $UpdateQuery = "
    UPDATE buyers SET
    orderstring='$temp'
    WHERE user='$user'";
  if($connection->query($UpdateQuery)===TRUE)
  { echo "Password Was name<br><br>"; } }

```

```

<?php
$result = queryMysql("SELECT * FROM buyers WHERE user='$user'");
if($result->num_rows !=0)
{
    while($rows = $result->fetch_assoc())
    {
        $fname = $rows['firstname'];
        echo"<li>
        <a href='userprofile.php'>Hello, $fname</a>";
    }
}

```

```

<?php
$result = queryMysql("SELECT * FROM buyers WHERE user='$user'");
if($result->num_rows !=0)
{
    while($rows = $result->fetch_assoc())
    {
        $reorderstring = $rows['orderstring'];
    }
}

```

```

$result = queryMysql("SELECT * FROM buyers WHERE user='$user'");
if($result->num_rows !=0)
{
    while($rows = $result->fetch_assoc())
    {
        $orderstring = $rows['orderstring'];
    }
}
if($orderstring != "00000000000000000000000000000000")
{
    $totalprice=0;
    $array =
    array(substr($orderstring,0,2),substr($orderstring,2,2),substr($orderstring,4,2),substr($orderstring,6,2),substr($orderstring,8,2),substr(
$orderstring,10,2),substr($orderstring,12,2),substr($orderstring,14,2),substr($orderstring,16,2),substr($orderstring,18,2),substr($orderst
ring,20,2),substr($orderstring,22,2));

    if($array[0]>0)
    {
        $resultt = queryMysql("SELECT * FROM items WHERE itemid='1'");
        $picture = mysqli_fetch_array($resultt);
        $price=number_format($picture['price'], 2, '.', '');
        $space=" ";
        echo '';
        echo '<p style="padding: 0px 200px 0px 0px" align="left">'. $picture[\'description\'] .\'</p>';          echo '<a align="right" class="btn
btn-default">Price: $ '. $price .\'</a><a>\' . $space .\'</a><a align="right" class="btn btn-default">Amount:  \' . $array[0] .\'</a>';
        $totalprice+=$price*$array[0];
        echo '<br><br><br><br>';
    }
    if($array[1]>0)
    {
        $resultt = queryMysql("SELECT * FROM items WHERE itemid='2'");
        $picture = mysqli_fetch_array($resultt);
        $price=number_format($picture['price'], 2, '.', '');
        $space=" ";
        echo '';
        echo '<p style="padding: 0px 200px 0px 0px" align="left">'. $picture[\'description\'] .\'</p>';          echo '<a align="right" class="btn
btn-default">Price: $ '. $price .\'</a><a>\' . $space .\'</a><a align="right" class="btn btn-default">Amount:  \' . $array[1] .\'</a>';
        $totalprice+=$price*$array[1];
        echo '<br><br><br><br>';
    }
    if($array[2]>0)
    {
        $resultt = queryMysql("SELECT * FROM items WHERE itemid='3'");

```

The screenshot above shows a portion of the functionality that repeats for all the items.

```

<?php

if(isset($_POST['submit']))
{
    echo "hasghajkghasklghaslkghasklgas";
    $timestamp = date('Y-m-d H:i:s');
    queryMysql("INSERT INTO orders VALUES('', '$user', '$orderstring', '$timestamp')");
    $string = "00000000000000000000000000000000";

    $sql=" UPDATE buyers SET
orderstring = '$string'
WHERE user='$user'";

    if($connection->query($sql)===TRUE){
        echo ("<SCRIPT LANGUAGE='JavaScript'>
window.alert('Order succesfully placed!')
window.location.href='http://lamp.cse.fau.edu/~mhus2015/ema11/index.php';
</SCRIPT>");
    }
    else{echo "Error updating record: ". $connection->error;}
}

?>

```

E-Mall app was created by two collaborators. All of the project features were done with evenly distributed workload and effort from both parties. We met on a daily basis for some period of time to work on the project. Both of the team members were working on the same parts of the project to make it more efficient and functional.