# CMPE 473 Project#1

Group#9

Abdullah Hanefi Önaldı

Ahmet Enes Bayraktar

# accept-bid.php

<?php

session\_start();

include('session.php');

$errmsg\_arr = array();

$errflag = false;

$itemID = $\_POST['itemID'];

$result = $conn->prepare("SELECT \* FROM item WHERE itemID = :itemID AND owner = :owner AND isSold = :isSold");

$result->execute(array(':itemID' => $itemID, ':owner' => $\_SESSION['username'], ':isSold' => 'no'));

$rows = $result->fetch(PDO::FETCH\_ASSOC);

if($rows > 0)

{

if($rows['bidder'] == "" && $rows['bidPrice'] == 0)

{

$errmsg\_arr[] = 'There is no bid to your item';

$errflag = true;

}

else

{

$result = $conn->prepare("UPDATE item SET price = :price, isSold = :isSold WHERE itemID = :itemID");

$result->execute(array(':itemID' => $itemID, ':price' => $rows['bidPrice'], ':isSold' => 'yes'));

header("location: sell-confirm.php");

}

}

else

{

$errmsg\_arr[] = 'Incorrect itemID';

$errflag = true;

}

if($errflag)

{

$\_SESSION['ERRMSG\_ARR'] = $errmsg\_arr;

session\_write\_close();

header("location: change-price.php");

exit();

}

?>

# bid-confirm.html

You have successfully bid the item.

<a href=home.php>Return to your home page</a><br>

# bid-confirm.php

<?php

session\_start();

include('session.php');

include('bid-confirm.html');

?>

# buy-confirm.html

You have successfully bought the item by paying its price.

<a href=home.php>Return to your home page</a><br>

# buy-confirm.php

<?php

session\_start();

include('session.php');

include('buy-confirm.html');

?>

# buy.php

<?php

session\_start();

include('session.php');

$errmsg\_arr = array();

$errflag = false;

$itemID = $\_POST['itemID'];

$result = $conn->prepare("SELECT \* FROM item WHERE itemID = :itemID AND isSold = :isSold");

$result->execute(array(':itemID' => $itemID, ':isSold' => 'no'));

$rows = $result->fetch(PDO::FETCH\_ASSOC);

if($rows > 0)

{

if($\_SESSION['username'] == $rows['owner'])

{

$errmsg\_arr[] = 'You can not buy your item';

$errflag = true;

}

else

{

$result = $conn->prepare("UPDATE item SET isSold = :isSold, bidder = :bidder, bidPrice = :bidPrice WHERE itemID = :itemID");

$result->execute(array(':itemID' => $itemID, ':isSold' => 'yes', ':bidder' => $\_SESSION['username'], ':bidPrice' => $rows['price']));

header("location: buy-confirm.php");

}

}

else

{

$errmsg\_arr[] = 'Incorrect itemID';

$errflag = true;

}

if($errflag)

{

$\_SESSION['ERRMSG\_ARR'] = $errmsg\_arr;

session\_write\_close();

header("location: buyout-bid.php");

exit();

}

?>

# buyout-bid.html

<a href=home.php>Home</a><br><br>

<form method="post" action="buyout-bid.php">

Search Tag:<input type="text" name="search">

<input type="submit" name="submit" value="Search">

</form>

<form method="post" action="change-data-bid.php">

Item ID:<input type="text" name="itemID">

Bid amount:<input type="text" name="bidPrice">

<input type="submit" name="submit" value="Bid">

</form>

<form method="post" action="buy.php">

Item ID:<input type="text" name="itemID">

<input type="submit" name="submit" value="Buyout">

</form>

<h2>Item List</h2>

<head>

<style>

table, th, td {

border: 1px solid black;

border-collapse: collapse;

}

th, td {

padding: 5px;

}

</style>

</head>

<body>

<table class="table table-bordered table-condensed">

<thead>

<tr>

<th>Name</th>

<th>Price</th>

<th>Current Bid</th>

<th>Bidder</th>

<th>Owner</th>

<th>ItemID</th>

<th>Description</th>

</tr>

</thead>

<tbody>

<?php

while ($r = $result->fetch())

{

echo "<tr>";

echo "<td>" . htmlspecialchars($r['name']) . "</td>";

echo "<td>" . htmlspecialchars($r['price']) . "</td>";

echo "<td>" . htmlspecialchars($r['bidPrice']) . "</td>";

echo "<td>" . htmlspecialchars($r['bidder']) . "</td>";

echo "<td>" . htmlspecialchars($r['owner']) . "</td>";

echo "<td>" . htmlspecialchars($r['itemID']) . "</td>";

echo "<td>" . "<textarea readonly>" . htmlspecialchars($r['description']) . "</textarea>" . "</td>";

echo "</tr>";

}

?>

</tbody>

</table>

</body>

# buyout-bid.php

<?php

session\_start();

include('session.php');

if(isset($\_SESSION['ERRMSG\_ARR']) && is\_array($\_SESSION['ERRMSG\_ARR']) && count($\_SESSION['ERRMSG\_ARR']) > 0)

{

echo '<ul style="padding:0; color:red;">';

foreach($\_SESSION['ERRMSG\_ARR'] as $msg)

{

echo '<li>' . $msg . '</li>';

}

echo '</ul>';

unset($\_SESSION['ERRMSG\_ARR']);

}

$search = "";

if($\_POST)

{

$search = $\_POST['search'];

}

$result = $conn->prepare("SELECT description, price, bidPrice, owner, itemID, name, isSold, bidder FROM item WHERE isSold = :isSold AND (name LIKE :search OR description LIKE :search) ORDER BY name");

$result->execute(array(':search' => '%' . $search . '%', ':isSold' => 'no'));

$result->setFetchMode(PDO::FETCH\_ASSOC);

include('buyout-bid.html');

?>

# chage-price-confirm.html

You have successfully changed the price of the item.

<a href=home.php>Return to your home page</a><br>

# chage-price-confirm.php

<?php

session\_start();

include('session.php');

include('change-price-confirm.html');

?>

# change-data-bid.php

<?php

session\_start();

include('session.php');

$errmsg\_arr = array();

$errflag = false;

$bidPrice = $\_POST['bidPrice'];

$bidder = $\_SESSION['username'];

$itemID = $\_POST['itemID'];

$result = $conn->prepare("SELECT \* FROM item WHERE itemID = :itemID AND isSold = :isSold");

$result->execute(array(':itemID' => $itemID, ':isSold' => 'no'));

$rows = $result->fetch(PDO::FETCH\_ASSOC);

if($rows > 0)

{

if($bidPrice >= $rows['price'])

{

$errmsg\_arr[] = 'You can not bid higher than price. You can buy instead.';

$errflag = true;

}

elseif($bidPrice <= $rows['bidPrice'])

{

$errmsg\_arr[] = 'You can not bid lower than the current bid.';

$errflag = true;

}

elseif($bidder == $rows['owner'])

{

$errmsg\_arr[] = 'You can not bid to your item.';

$errflag = true;

}

else

{

$result = $conn->prepare("UPDATE item SET bidPrice = :bidPrice, bidder = :bidder WHERE itemID = :itemID");

$result->execute(array(':bidPrice' => $bidPrice, ':bidder' => $bidder, ':itemID' => $itemID));

header("location: bid-confirm.php");

}

}

else

{

$errmsg\_arr[] = 'Incorrect itemID';

$errflag = true;

}

if($errflag)

{

$\_SESSION['ERRMSG\_ARR'] = $errmsg\_arr;

session\_write\_close();

header("location: buyout-bid.php");

exit();

}

?>

# change-data-item.php

<?php

session\_start();

include('session.php');

$errmsg\_arr = array();

$errflag = false;

$name = $\_POST['name'];

$itemID = $\_POST['itemID'];

$description = $\_POST['description'];

$result = $conn->prepare("SELECT \* FROM item WHERE itemID = :itemID AND isSold = :isSold AND owner = :owner");

$result->execute(array(':itemID' => $itemID, ':isSold' => 'no', ':owner' => $\_SESSION['username']));

$rows = $result->fetch(PDO::FETCH\_ASSOC);

if($rows > 0)

{

if($name == "")

{

$name = $rows['name'];

}

if($description == "")

{

$description == $rows['description'];

}

$result = $conn->prepare("UPDATE item SET name = :name, description = :description WHERE itemID = :itemID");

$result->execute(array(':name' => $name, ':description' => $description, ':itemID' => $itemID));

header("location: edit-confirm.php");

}

else

{

$errmsg\_arr[] = 'Incorrect itemID or item is sold';

$errflag = true;

}

if($errflag)

{

$\_SESSION['ERRMSG\_ARR'] = $errmsg\_arr;

session\_write\_close();

header("location: change-price.php");

exit();

}

?>

# change-data-price.php

<?php

session\_start();

include('session.php');

$errmsg\_arr = array();

$errflag = false;

$newPrice = $\_POST['newPrice'];

$itemID = $\_POST['itemID'];

$result = $conn->prepare("SELECT \* FROM item WHERE itemID = :itemID AND owner = :owner AND isSold = :isSold");

$result->execute(array(':itemID' => $itemID, ':owner' => $\_SESSION['username'], 'isSold' => 'no'));

$rows = $result->fetch(PDO::FETCH\_ASSOC);

if($rows > 0)

{

if($newPrice <= $rows['bidPrice'])

{

$errmsg\_arr[] = 'Price can not be equal or lower than bid price. You can accept its bid instead.';

$errflag = true;

}

else

{

$result = $conn->prepare("UPDATE item SET price = :newPrice WHERE itemID = :itemID");

$result->execute(array(':newPrice' => $newPrice, ':itemID' => $itemID));

header("location: change-price-confirm.php");

}

}

else

{

$errmsg\_arr[] = 'Incorrect itemID';

$errflag = true;

}

if($errflag)

{

$\_SESSION['ERRMSG\_ARR'] = $errmsg\_arr;

session\_write\_close();

header("location: change-price.php");

exit();

}

?>

# change-price.html

<a href=home.php>Home</a><br><br>

<form method="post" action="change-price.php">

Search Tag:<input type="text" name="search">

<input type="submit" name="submit" value="Search">

</form>

<form method="post" action="change-data-price.php">

Item ID:<input type="text" name="itemID">

New Price:<input type="text" name="newPrice">

<input type="submit" name="submit" value="Change Price">

</form>

<form method="post" action="accept-bid.php">

Item ID:<input type="text" name="itemID">

<input type="submit" name="submit" value="Accept Bid">

</form>

<form method="post" action="delete.php">

Item ID:<input type="text" name="itemID">

<input type="submit" name="submit" value="Delete">

</form>

<form method="post" action="change-data-item.php">

Edit Item:<br>

Choose Item ID:<input type="text" name="itemID">

<br>

Name:<input type="text" name="name">

Description:<input type="text" name="description">

<input type="submit" name="submit" value="Edit">

</form>

<h2>Item List</h2>

<head>

<style>

table, th, td {

border: 1px solid black;

border-collapse: collapse;

}

th, td {

padding: 5px;

}

</style>

</head>

<body>

<table class="table table-bordered table-condensed">

<thead>

<tr>

<th>Name</th>

<th>Price</th>

<th>Current Bid</th>

<th>Owner</th>

<th>ItemID</th>

<th>Bidder</th>

<th>Sold</th>

<th>Description</th>

</tr>

</thead>

<tbody>

<?php

while ($r = $result->fetch())

{

echo "<tr>";

echo "<td>" . htmlspecialchars($r['name']) . "</td>";

echo "<td>" . htmlspecialchars($r['price']) . "</td>";

echo "<td>" . htmlspecialchars($r['bidPrice']) . "</td>";

echo "<td>" . htmlspecialchars($r['owner']) . "</td>";

echo "<td>" . htmlspecialchars($r['itemID']) . "</td>";

echo "<td>" . htmlspecialchars($r['bidder']) . "</td>";

echo "<td>" . htmlspecialchars($r['isSold']) . "</td>";

echo "<td>" . "<textarea readonly>" . htmlspecialchars($r['description']) . "</textarea>" . "</td>";

echo "</tr>";

}

?>

</tbody>

</table>

</body>

# change-price.php

<?php

session\_start();

include('session.php');

if(isset($\_SESSION['ERRMSG\_ARR']) && is\_array($\_SESSION['ERRMSG\_ARR']) && count($\_SESSION['ERRMSG\_ARR']) > 0)

{

echo '<ul style="padding:0; color:red;">';

foreach($\_SESSION['ERRMSG\_ARR'] as $msg)

{

echo '<li>',$msg,'</li>';

}

echo '</ul>';

unset($\_SESSION['ERRMSG\_ARR']);

}

$search = "";

if($\_POST)

{

$search = $\_POST['search'];

}

$result = $conn->prepare("SELECT description, price, bidPrice, owner, itemID, name, bidder, isSold FROM item WHERE owner = :owner AND (name LIKE :search OR description LIKE :search) ORDER BY name");

$result->execute(array(':search' => '%' . $search . '%', ':owner' => $\_SESSION['username']));

$result->setFetchMode(PDO::FETCH\_ASSOC);

include('change-price.html');

?>

# delete-confirm.html

You have successfully deleted the item.

<a href=home.php>Return to your home page</a><br>

# delete-confirm.php

<?php

session\_start();

include('session.php');

include('delete-confirm.html');

?>

# delete.php

<?php

session\_start();

include('session.php');

$errmsg\_arr = array();

$errflag = false;

$itemID = $\_POST['itemID'];

$result = $conn->prepare("SELECT \* FROM item WHERE itemID = :itemID AND owner = :owner");

$result->execute(array(':itemID' => $itemID, ':owner' => $\_SESSION['username']));

$rows = $result->fetch(PDO::FETCH\_ASSOC);

if($rows > 0)

{

$result = $conn->prepare("DELETE FROM item WHERE itemID = :itemID");

$result->execute(array(':itemID' => $itemID));

header("location: delete-confirm.php");

}

else

{

$errmsg\_arr[] = 'Incorrect itemID';

$errflag = true;

}

if($errflag)

{

$\_SESSION['ERRMSG\_ARR'] = $errmsg\_arr;

session\_write\_close();

header("location: change-price.php");

exit();

}

?>

# edit-confirm.html

You have successfully edit the item.

<a href=home.php>Return to your home page</a><br>

# edit-confirm.php

<?php

session\_start();

include('session.php');

include('edit-confirm.html');

?>

# home.html

<a href=buyout-bid.php>Buyout or Bid</a><br>

<a href=sell.php>Sell an Item</a><br>

<a href=change-price.php>Your Items</a><br>

<a href=logout.php>Log out</a>

# home.php

<?php

session\_start();

include('session.php');

include('home.html');

?>

# index.html

<form action="index.php" method="POST">

Username<br>

<input type="text" name="uname" /><br>

Password<br>

<input type="password" name="pword" /><br>

<input type="submit" value="Login" />

<a href=register.php>Click Here to Register</a>

</form>

# index.php

<?php

session\_start();

if( isset($\_SESSION['ERRMSG\_ARR']) && is\_array($\_SESSION['ERRMSG\_ARR']) && count($\_SESSION['ERRMSG\_ARR']) > 0)

{

echo '<ul style="padding:0; color:red;">';

foreach($\_SESSION['ERRMSG\_ARR'] as $msg)

{

echo '<li>',$msg,'</li>';

}

echo '</ul>';

unset($\_SESSION['ERRMSG\_ARR']);

}

include('index.html');

if($\_POST)

{

$errmsg\_arr = array();

$errflag = false;

$username = $\_POST['uname'];

$password = $\_POST['pword'];

if($username == '')

{

$errmsg\_arr[] = 'You must enter your Username';

$errflag = true;

}

if($password == '')

{

$errmsg\_arr[] = 'You must enter your Password';

$errflag = true;

}

if($errflag)

{

$\_SESSION['ERRMSG\_ARR'] = $errmsg\_arr;

session\_write\_close();

header("location: index.php");

exit();

}

$dbhost = "localhost";

$dbname = "auction house";

$dbuser = "root";

$dbpass = "1234";

$conn = new PDO("mysql:host=$dbhost;dbname=$dbname",$dbuser,$dbpass);

$result = $conn->prepare("SELECT \* FROM user WHERE username= :username AND password= :password");

$result->bindParam(':username', $username);

$result->bindParam(':password', $password);

$result->execute();

$rows = $result->fetch(PDO::FETCH\_NUM);

if($rows > 0)

{

$\_SESSION['username'] = $username;

header("location: home.php");

}

else

{

$errmsg\_arr[] = 'Username and Password are not correct';

$errflag = true;

}

if($errflag)

{

$\_SESSION['ERRMSG\_ARR'] = $errmsg\_arr;

session\_write\_close();

header("location: index.php");

exit();

}

}

?>

# logout.php

<?php

session\_start();

if(session\_destroy())

{

header("Location: index.php");

}

?>

# register.html

<a href=index.php>Login Page</a><br>

<form action="register.php" method="POST">

Username<br>

<input type="text" name="uname" /><br>

Password<br>

<input type="text" name="pword" /><br>

Confirm Password<br>

<input type="text" name="cpword" /><br>

<input type="submit" value="Register" />

</form>

# register.php

<?php

session\_start();

if( isset($\_SESSION['ERRMSG\_ARR']) && is\_array($\_SESSION['ERRMSG\_ARR']) && count($\_SESSION['ERRMSG\_ARR']) > 0)

{

echo '<ul style="padding:0; color:red;">';

foreach($\_SESSION['ERRMSG\_ARR'] as $msg)

{

echo '<li>',$msg,'</li>';

}

echo '</ul>';

unset($\_SESSION['ERRMSG\_ARR']);

}

if($\_POST)

{

$errmsg\_arr = array();

$errflag = false;

$username = $\_POST['uname'];

$password = $\_POST['pword'];

$cpassword = $\_POST['cpword'];

if($username == '')

{

$errmsg\_arr[] = 'You must enter your Username';

$errflag = true;

}

elseif(!preg\_match("/^[a-zA-Z0-9.\S]+$/",$username))

{

$errmsg\_arr[] = 'Username must contain only numbers and letters';

$errflag = true;

}

if($password == '')

{

$errmsg\_arr[] = 'You must enter your Password';

$errflag = true;

}

elseif(!preg\_match("/^[\S]+$/",$password))

{

$errmsg\_arr[] = 'Password must not contain spaces';

$errflag = true;

}

elseif($cpassword == '')

{

$errmsg\_arr[] = 'You must enter Confirm Password';

$errflag = true;

}

elseif($password != $cpassword)

{

$errmsg\_arr[] = 'Your password must match';

$errflag = true;

}

if($errflag)

{

$\_SESSION['ERRMSG\_ARR'] = $errmsg\_arr;

session\_write\_close();

header("location: register.php");

exit();

}

$dbhost = "localhost";

$dbname = "auction house";

$dbuser = "root";

$dbpass = "1234";

$conn = new PDO("mysql:host=$dbhost;dbname=$dbname",$dbuser,$dbpass);

$result = $conn->prepare("SELECT \* FROM user WHERE username= :username");

$result->bindParam(':username', $username);

$result->execute();

$rows = $result->fetch(PDO::FETCH\_NUM);

if($rows > 0)

{

$errmsg\_arr[] = 'Username already exists';

$errflag = true;;

}

if($errflag)

{

$\_SESSION['ERRMSG\_ARR'] = $errmsg\_arr;

session\_write\_close();

header("location: register.php");

exit();

}

$sql = "INSERT INTO user (username, password) VALUES (:username,:password)";

$q = $conn->prepare($sql);

$q->execute(array(':username'=>$username,':password'=>$password));

header("location: index.php");

}

include('register.html');

?>

# sell-confirm.html

You have successfully sold the item from the current bid.

<a href=home.php>Return to your home page</a><br>

# sell-confirm.php

<?php

session\_start();

include('session.php');

include('sell-confirm.html');

?>

# sell-listed.html

You have successfully added the item to the item list.

<a href=home.php>Return to your home page</a><br>

# sell-listed.php

<?php

session\_start();

include('session.php');

include('sell-listed.html');

?>

# sell.html

<a href=home.php>Home</a><br>

<h2>Item Form</h2>

<form method="post" action="sell.php">

Name of the item: <input type="text" name="name">

<br>

Price of the item: <input type="text" name="price">

<br><br>

Description of the item: <textarea name="description" rows="5" cols="40"></textarea>

<br><br>

<input type="submit" name="submit" value="Submit">

</form>

# sell.php

<?php

session\_start();

include('session.php');

if(isset($\_SESSION['ERRMSG\_ARR']) && is\_array($\_SESSION['ERRMSG\_ARR']) && count($\_SESSION['ERRMSG\_ARR']) > 0)

{

echo '<ul style="padding:0; color:red;">';

foreach($\_SESSION['ERRMSG\_ARR'] as $msg)

{

echo '<li>',$msg,'</li>';

}

echo '</ul>';

unset($\_SESSION['ERRMSG\_ARR']);

}

if($\_POST)

{

$errmsg\_arr = array();

$errflag = false;

$name = $\_POST['name'];

$price = $\_POST['price'];

$description = $\_POST['description'];

if($name == "")

{

$errmsg\_arr[] = "Name is required";

$errflag = true;

}

elseif(!preg\_match("/^[a-zA-Z0-9]/",$name))

{

$errflag = true;

$errmsg\_arr[] = "Name can contain characters and numbers";

}

if($price == "")

{

$errmsg\_arr[] = "Price is required";

$errflag = true;

}

elseif(!is\_numeric($price))

{

$errmsg\_arr[] = "Price has to be number";

$errflag = true;

}

elseif($price < 0)

{

$errmsg\_arr[] = "Price has to be positive number";

$errflag = true;

}

if($description == "")

{

$errmsg\_arr[] = "Decription is required";

$errflag = true;

}

if($errflag)

{

$\_SESSION['ERRMSG\_ARR'] = $errmsg\_arr;

session\_write\_close();

header("location: sell.php");

exit();

}

$sql = "INSERT INTO item (description, price, owner, name) VALUES (:description,:price,:own,:name)";

$q = $conn->prepare($sql);

$q->execute(array(':description'=>$description,':price'=>$price,':own'=>$\_SESSION['username'], ':name' => $name));

header("location: sell-listed.php");

}

include('sell.html');

?>

# session.php

<?php

$dbhost = "localhost";

$dbname = "auction house";

$dbuser = "root";

$dbpass = "1234";

$conn = new PDO("mysql:host=$dbhost;dbname=$dbname", $dbuser, $dbpass);

$username=$\_SESSION['username'];

if(!isset($username))

{

$conn = null;

header('Location: index.php');

}

?>