**Source code files for the Storefront project:**

**add\_product.php**

<?php

$page\_title = 'Add Product';

include ('../includes/header.php');

require "../config.php";

echo '<div class="page-header"><h2><b>Add Product</b></h2></div>';

//Deny access to any non-admin

if (!isset($\_SESSION['admin']) || $\_SESSION['admin'] !== true) {

echo '<h4 class="error text-center">Error: Access denied</h4>';

exit;

}

if ($\_SERVER['REQUEST\_METHOD'] == 'POST') { //Handle post form

//Check if all fields have an input

if (!empty($\_POST['product\_name']) && !empty($\_POST['description']) && !empty($\_POST['price']) && !empty($\_POST['image']) ) {

//Trim inputs

$pn = trim($\_POST['product\_name']);

$desc = trim($\_POST['description']);

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

$color = trim($\_POST['color']);

$price = trim($\_POST['price']);

$img = trim($\_POST['image']);

//Add product to database

$q = 'INSERT INTO entity\_product (product\_name, description, type, product\_color, product\_price, image) VALUES (?, ?, ?, ?, ?, ?)';

$stmt = mysqli\_prepare($link, $q);

mysqli\_stmt\_bind\_param($stmt, 'ssssss', $pn, $desc, $type, $color, $price, $img);

mysqli\_stmt\_execute($stmt);

//Check results

if (mysqli\_stmt\_affected\_rows($stmt) == 1) {

echo '<p class="text-center" style="color:green;">The product has been added.</p>';

$\_POST = array();

} else {

$error = 'The product could not be added to the database.';

}

//Close prepared statement

mysqli\_stmt\_close($stmt);

} else {

$error = 'Please enter all fields'; //Error message

}

}

// Check for an error and print it:

if (isset($error)) {

echo '<div class="text-center">

<h1>Error!</h1>

<p style="font-weight:bold; color:#C00">' . $error . '</p>

</div>';

}

?>

<div class="form">

<form action="add\_product.php" method="post">

<p>Product Name: <input type="text" name="product\_name"></p>

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

<?php

//Query for product types

$qType = "SELECT \* FROM `storefront`.`enum\_product\_type` AS `enum\_product\_type`";

$rsType = mysqli\_query($link, $qType);

$numType = mysqli\_num\_rows($rsType); //Total number of product types

echo '<p>Type: <select name="type">';

//Select box for product type

for ($i=0; $i<$numType; $i++) {

mysqli\_data\_seek($rsType, $i);

$rowType = $rsType->fetch\_assoc();

//Output product types as a drop down list, default select the original product type

echo '<option value="' . ($i+1) . '">' . $rowType['product\_type'] . '</option>';

}

echo '</select>';

?>

<p>Color: <input type="text" name="color"></p>

<p>Price: <input type="text" name="price"></p>

<p>Image: <input type="text" name="image"></p>

<div class="text-center"> <input type="submit" name="submit" value="Add"></div>

</form>

</div>

<div class="text-center">

<a href="inventory.php" class="btn btn-secondary">Go back to Inventory</a>

</div>

</body>

</html>

**add\_product\_variant.php**

<?php

$page\_title = 'Add Product Variant';

include ('../includes/header.php');

require "../config.php";

echo '<div class="page-header"><h2><b>Add Product Variant</b></h2></div>';

//Check admin status

if (!isset($\_SESSION['admin']) || $\_SESSION['admin'] !== true) {

echo '<h4 class="error text-center">Error: Access denied</h4>';

exit;

}

//Check for a valid user ID, through GET or POST:

if ( (isset($\_GET['id'])) && (is\_numeric($\_GET['id'])) ) {

$id = $\_GET['id'];

} elseif ( (isset($\_POST['id'])) && (is\_numeric($\_POST['id'])) ) { //Form submission

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

} else { //No valid ID, kill script

echo '<h4 class="error text-center">Error: Product variant not found</h4>';

exit;

}

//For form submission

if ($\_SERVER['REQUEST\_METHOD'] == 'POST') {

//Check if all fields have an input

if (!empty($\_POST['size']) && !empty($\_POST['quantity'])) {

//Trim inputs

$size = trim($\_POST['size']); //Get size from form as: XS, S, M, L, XL, etc...

$qty = trim($\_POST['quantity']);

//Convert the size and check if the enum\_size table contains it

$qSz = "SELECT `size\_id`, `size` FROM `storefront`.`enum\_size` AS `enum\_size` WHERE `size` = '$size'";

$rSz = mysqli\_query($link, $qSz);

//If query successful

if (mysqli\_num\_rows($rSz) == 1) {

$row = mysqli\_fetch\_array($rSz, MYSQLI\_NUM);

$sizeInt = $row[0]; //Size as an integer (Ex: Input XL -> Output 6)

// Add product to database

$q = "INSERT INTO entity\_product\_variant (variant\_size, variant\_quantity) VALUES (?, ?)";

$stmt = mysqli\_prepare($link, $q);

mysqli\_stmt\_bind\_param($stmt, 'ss', $sizeInt, $qty);

mysqli\_stmt\_execute($stmt);

//Check results

if (mysqli\_stmt\_affected\_rows($stmt) == 1) {

//Add to xref\_product\_variant\_product

$variant\_id = mysqli\_insert\_id($link);

$q2 = "INSERT INTO xref\_product\_variant\_product (product\_id, product\_variant\_id) VALUES (?, ?)";

$stmt2 = mysqli\_prepare($link, $q2);

mysqli\_stmt\_bind\_param($stmt2, 'ss', $id, $variant\_id);

mysqli\_stmt\_execute($stmt2);

mysqli\_stmt\_close($stmt2);

//Output message

echo '<p class="text-center" style="color:green;">The product variant has been added.</p>';

} else { //Error occurred

$error = 'The product variant could not be added to the database.';

}

mysqli\_stmt\_close($stmt); //Close prepared statement

}

else {

echo '<h4 class="error text-center">Please enter a valid size. If not sure, please look at manual.</h4>';

}

} else {

$error = 'Please enter all fields'; //Error message

}

}

// Check for an error and print it:

if (isset($error)) {

echo '<p class="error text-center">Error: ' . $error . '</p>';

}

$query = "SELECT `entity\_product`.`product\_id`, `entity\_product`.`product\_name`, `entity\_product`.`description`, `enum\_product\_type`.`product\_type`, `entity\_product`.`product\_color`, `entity\_product`.`product\_price` FROM `storefront`.`entity\_product` AS `entity\_product`, `storefront`.`enum\_product\_type` AS `enum\_product\_type` WHERE `entity\_product`.`type` = `enum\_product\_type`.`id` AND `entity\_product`.`product\_id` = $id";

$rs = mysqli\_query($link, $query);

echo "<div class='text-center'>";

echo "<table border='1' class='tcenter'>";

echo "<tr><th>" . 'Name' . "</th>";

echo "<th>" . 'Description' . "</th>";

echo "<th>" . 'Type' . "</th>";

echo "<th>" . 'Color' . "</th>";

echo "<th>" . 'Price' . "</th>";

while($re = mysqli\_fetch\_array($rs, MYSQLI\_BOTH)) {

echo "<tr><td>" . $re['product\_name'] . "</td>";

echo "<td>" . $re['description'] . "</td>";

echo "<td>" . $re['product\_type'] . "</td>";

echo "<td>" . $re['product\_color'] . "</td>";

echo "<td>" . $re['product\_price'] . "</td></tr>";

}

echo "</table>";

echo "</div>";

?>

<div class="form">

<form action="add\_product\_variant.php" method="post">

<p>Size: <input type="text" name="size"></p>

<p>Quantity: <input type="text" name ="quantity"></p>

<div class="text-center"> <input type="submit" name="submit" value="Add Variant"></div>

<?php echo '<input type="hidden" name="id" value="' . $id . '">'; ?>

</form>

</div>

<div class="text-center">

<a href="inventory.php" class="btn btn-secondary">Go back to Inventory</a>

</div>

</body>

</html>

**admin.php**

<?php

$page\_title = 'Admin Panel';

include ('../includes/header.php');

require\_once "../config.php";

echo '<div class="page-header"><h2><b>Admin Panel</b></h2></div>';

//Deny access to any non-admin

if (!isset($\_SESSION['admin']) || $\_SESSION['admin'] !== true) {

echo '<h4 class="error text-center">Error: Access denied</h4>';

exit;

}

?>

<div class="text-center">

<a href="inventory.php" style="width:150px;" class="btn btn-primary">View Inventory</a><br><br>

<a href="view\_user.php" style="width:150px;" class="btn btn-info">View Users</a><br><br>

<div class="settings">

<h3><span class="glyphicon glyphicon-cog"></span> Settings</h3>

<a href="../reset\_password.php" class="btn btn-warning">Reset password</a>

</div>

</div>

</body>

</html>

**delete\_product.php**

<?php

$page\_title = 'Delete Product';

include ('../includes/header.php');

require\_once "../config.php";

echo '<div class="page-header"><h2><b>Delete Product</b></h2></div>';

//Check admin status

if (!isset($\_SESSION['admin']) || $\_SESSION['admin'] !== true) {

echo '<h4 class="error text-center">Error: Access denied</h4>';

exit;

}

//Check for a valid product ID, through GET or POST

if ( (isset($\_GET['id'])) && (is\_numeric($\_GET['id'])) ) {

$id = $\_GET['id'];

} elseif ( (isset($\_POST['id'])) && (is\_numeric($\_POST['id'])) ) {

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

} else { //No valid ID, kill script

echo '<h4 class="error text-center">Error: Product not found</h4>';

exit;

}

//Only if form has been submitted on the page

if ($\_SERVER['REQUEST\_METHOD'] == 'POST') {

//Delete record if yes is chosen

if ($\_POST['sure'] == 'Yes') {

//Delete any xref for the product

$q = "DELETE FROM xref\_product\_variant\_product WHERE product\_id = $id";

mysqli\_query($link, $q);

//Delete product\_variant for the product

$q2 = "DELETE FROM entity\_product\_variant WHERE product\_id = $id";

mysqli\_query($link, $q2);

//Delete the product itself

$q3 = "DELETE FROM entity\_product WHERE product\_id = $id LIMIT 1";

mysqli\_query ($link, $q3);

echo '<div class="text-center">';

echo '<h4 style="color:green;">The product has been deleted.</h4>';

echo '</div>';

} else {

echo '<div class="text-center">';

echo '<p>The product has NOT been deleted.</p>';

echo '</div>';

}

echo '<div class="text-center">

<a href="inventory.php" class="btn btn-secondary">Go back to Inventory</a>

</div>';

}

else { //Show form

$sql = "SELECT `entity\_product`.\*, `enum\_product\_type`.`product\_type`, `entity\_product`.`product\_id` FROM `storefront`.`entity\_product` AS `entity\_product`, `storefront`.`enum\_product\_type` AS `enum\_product\_type` WHERE `entity\_product`.`type` = `enum\_product\_type`.`id` AND `entity\_product`.`product\_id` = $id";

$rs = mysqli\_query($link,$sql);

if (mysqli\_num\_rows($rs) == 1) {

//Get product information

$row = mysqli\_fetch\_array ($rs, MYSQLI\_NUM);

//Display the record being deleted

echo "<div class='text-center'>";

echo "<h3>Product name: $row[1]</h3>

<h3>Description: $row[2]</h3>

<h3>Type: $row[7]</h3>

<h3>Price: $$row[5]</h3>

</div>";

//Create the form

echo '<div class="form">

<p>Are you sure you want to delete this product?</p>

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

<input type="radio" name="sure" value="Yes"> Yes

<input type="radio" name="sure" value="No" style="margin-left:10px;" checked="checked"> No<br><br>

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

<input type="hidden" name="id" value="' . $id . '">

</form>';

echo "</div>";

echo '<div class="text-center">

<a href="inventory.php" class="btn btn-secondary">Go back to Inventory</a>

</div>';

} else { //Access error

echo '<p class="error text-center">This page has been accessed in error.</p>';

}

}

?>

**delete\_product\_variant.php**

<?php

$page\_title = 'Delete Product Variant';

include ('../includes/header.php');

require\_once "../config.php";

echo '<div class="page-header"><h2><b>Delete Product Variant</b></h2></div>';

//Check admin status

if (!isset($\_SESSION['admin']) || $\_SESSION['admin'] !== true) {

echo '<h4 class="error text-center">Error: Access denied</h4>';

exit;

}

//Check for a valid product ID, through GET or POST

if ( (isset($\_GET['id\_1'])) && (is\_numeric($\_GET['id\_1'])) && (isset($\_GET['id\_2'])) && (is\_numeric($\_GET['id\_2'])) ) {

$id1 = $\_GET['id\_1'];

$id2 = $\_GET['id\_2'];

} elseif ( (isset($\_POST['id\_1'])) && (is\_numeric($\_POST['id\_1'])) && (isset($\_POST['id\_2'])) && (is\_numeric($\_POST['id\_2'])) ) {

$id1 = $\_POST['id\_1'];

$id2 = $\_POST['id\_2'];

} else { //No valid ID, kill script

echo '<h4 class="error text-center">Error: Product variant not found</h4>';

exit;

}

//Only if form has been submitted on the page

if ($\_SERVER['REQUEST\_METHOD'] == 'POST') {

//Delete record if yes is chosen

if ($\_POST['sure'] == 'Yes') {

//Delete any xref for the product variant

$q = "DELETE FROM xref\_product\_variant\_product WHERE product\_variant\_id = $id2";

mysqli\_query($link, $q);

//Delete the product variant

$q2 = "DELETE FROM entity\_product\_variant WHERE variant\_id = $id2";

mysqli\_query($link, $q2);

echo '<div class="text-center">';

echo '<p class="text-center" style="color:green;">The product variant has been deleted.</p>';

echo '</div>';

} else {

echo '<div class="text-center">';

echo '<p>The product variant has NOT been deleted.</p>';

echo '</div>';

}

echo '<div class="text-center">

<a href="inventory.php" class="btn btn-secondary">Go back to Inventory</a>

</div>';

}

else { //Show form

$sql = "SELECT `entity\_product`.`product\_id`, `entity\_product\_variant`.`variant\_id`, `entity\_product`.`product\_name`, `enum\_size`.`size`, `entity\_product\_variant`.`variant\_quantity` FROM `storefront`.`entity\_product` AS `entity\_product`, `storefront`.`enum\_product\_type` AS `enum\_product\_type`, `storefront`.`entity\_product\_variant` AS `entity\_product\_variant`, `storefront`.`enum\_size` AS `enum\_size`, `storefront`.`xref\_product\_variant\_product` AS `xref\_product\_variant\_product` WHERE `entity\_product`.`type` = `enum\_product\_type`.`id` AND `entity\_product\_variant`.`variant\_size` = `enum\_size`.`size\_id` AND `xref\_product\_variant\_product`.`product\_id` = `entity\_product`.`product\_id` AND `xref\_product\_variant\_product`.`product\_variant\_id` = `entity\_product\_variant`.`variant\_id` AND `entity\_product`.`product\_id` = $id1 AND `entity\_product\_variant`.`variant\_id` = $id2";

$rs = mysqli\_query($link,$sql);

if (mysqli\_num\_rows($rs) == 1) {

//Get product information

$row = mysqli\_fetch\_array ($rs, MYSQLI\_NUM);

//Display the record being deleted

echo "<div class='text-center'>

<h3>Product name: $row[2]</h3>

<h3>Size: $row[3]</h3>

<h3>Quantity: $row[4]</h3>

</div>";

//Create the form

echo '<div class="form">

<p>Are you sure you want to delete this product variant?</p>

<form action="delete\_product\_variant.php" method="post">

<input type="radio" name="sure" value="Yes"> Yes

<input type="radio" name="sure" value="No" style="margin-left:10px;" checked="checked"> No<br><br>

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

<input type="hidden" name="id\_1" value="' . $id1 . '">

<input type="hidden" name="id\_2" value="' . $id2 . '">

</form>';

echo "</div>";

echo '<div class="text-center">

<a href="inventory.php" class="btn btn-secondary">Go back to Inventory</a>

</div>';

} else { //Access error

echo '<p class="error text-center">This page has been accessed in error.</p>';

}

}

mysqli\_close($link);

?>

**delete\_user.php**

<?php

$page\_title = 'Delete User';

include ('../includes/header.php');

require ('../config.php');

echo '<div class="page-header"><h2><b>Delete User</b></h2></div>';

//Check admin status

if (!isset($\_SESSION['admin']) || $\_SESSION['admin'] !== true) {

echo '<h4 class="error text-center">Error: Access denied</h4>';

exit;

}

//Check for a valid user ID, through GET or POST

if ( (isset($\_GET['id'])) && (is\_numeric($\_GET['id'])) ) {

$id = $\_GET['id'];

} elseif ( (isset($\_POST['id'])) && (is\_numeric($\_POST['id'])) ) {

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

} else {

echo '<h4 class="error text-center">Error: Unable to find user</h4>';

exit;

}

?>

<div class="page-header">

<h1><b>Delete user</b></h1>

</div>

<?php

//Check if form has been submitted

if ($\_SERVER['REQUEST\_METHOD'] == 'POST') {

if ($\_POST['sure'] == 'Yes') {

//Delete xrefs with foreign keys first

$q = "DELETE FROM xref\_user\_order WHERE user\_id = $id";

mysqli\_query($link, $q);

//Delete user

$q2 = "DELETE FROM entity\_user WHERE user\_id = $id LIMIT 1";

$r = mysqli\_query ($link, $q2);

//If deletion is successful

if (mysqli\_affected\_rows($link) == 1) {

echo '<div class="text-center">

<p>The user has been deleted.</p>

<a href="view\_user.php" class="btn btn-secondary">Go back</button>

</div>';

} else {

echo '<div class="text-center">

<p class="error">The user could not be deleted due to a system error.</p>

<p>' . mysqli\_error($link) . '<br />Query: ' . $q . '</p>

<a href="view\_user.php" class="btn btn-secondary">Go back</button>

</div>';

}

} else {

echo '<div class="text-center">

<p>The user has NOT been deleted.</p>

<a href="view\_user.php" class="btn btn-secondary">Go back</button>

</div>';

}

}

//Show form

else {

//Retrieve the user's information

$query = "SELECT \* FROM entity\_user WHERE user\_id= '$id'";

$rs = mysqli\_query ($link, $query);

//If query is successful

if (mysqli\_num\_rows($rs) == 1) {

// Get the user's information:

$row = mysqli\_fetch\_array($rs, MYSQLI\_NUM);

$accType = ($row[6] == 0) ? "Admin" : "User"; //Get user account type

// Display the record being deleted:

echo "<div class='text-center'>

<h3>Email: $row[1]</h3>

<h3>Name: $row[3] $row[4]</h3>

<h3>Account type: $accType</h3>

</div>";

// Create the form:

echo '<div class="form">

<p>Are you sure you want to delete this user?</p>

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

<input type="radio" name="sure" value="Yes" /> Yes

<input type="radio" name="sure" value="No" style="margin-left:10px;" checked="checked" /> No<br><br>

<input type="submit" class="center" name="submit" value="Submit" />

<input type="hidden" name="id" value="' . $id . '" />

</form>

</div>';

echo '<div class="text-center">

<a href="view\_user.php" class="btn btn-secondary">Go back to Users</a>

</div>';

} else { //Not a valid user ID

echo '<p class="error">This page has been accessed in error.</p>';

}

}

mysqli\_close($link);

?>

**edit\_product.php**

<?php

$page\_title = 'Edit Product';

include ('../includes/header.php');

require\_once "../config.php";

echo '<div class="page-header"><h2><b>Edit Product</b></h2></div>';

//Check admin status

if (!isset($\_SESSION['admin']) || $\_SESSION['admin'] !== true) {

echo '<h4 class="error text-center">Error: Access denied</h4>';

exit;

}

//Check for a valid user ID, through GET or POST:

if ( (isset($\_GET['id'])) && (is\_numeric($\_GET['id'])) ) {

$id = $\_GET['id'];

} elseif ( (isset($\_POST['id'])) && (is\_numeric($\_POST['id'])) ) { //Form submission

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

} else { //No valid ID, kill script

echo '<h4 class="error text-center">Error: Produc tnot found</h4>';

exit;

}

//Check if the form has been submitted

if ($\_SERVER['REQUEST\_METHOD'] == 'POST') {

$errors = array(); //To hold errors

//Check product name

if (empty($\_POST['product\_name'])) {

$errors[] = 'Please enter product name.';

} else {

$pn = mysqli\_real\_escape\_string($link, trim($\_POST['product\_name']));

}

//Check description

if (empty($\_POST['description'])) {

$errors[] = 'Please enter a description.';

} else {

$desc = mysqli\_real\_escape\_string($link, trim($\_POST['description']));

}

//Check color

if (empty($\_POST['color'])) {

$errors[] = 'Please enter a color.';

} else {

$color = mysqli\_real\_escape\_string($link, trim($\_POST['color']));

}

//Check price

if (empty($\_POST['price'])) {

$errors[] = 'Please enter a price.';

} else {

$price = mysqli\_real\_escape\_string($link, trim($\_POST['price']));

}

//Get type selected

$type = mysqli\_real\_escape\_string($link, trim($\_POST['type']));

//Check Image

if (empty($\_POST['image'])) {

$errors[] = 'Please enter a image file.';

} else {

$image = mysqli\_real\_escape\_string($link, trim($\_POST['image']));

}

//If no errors

if (empty($errors)) {

// Make the query:

$q = "UPDATE entity\_product SET product\_name='$pn', description='$desc', product\_price='$price', product\_color='$color', type='$type', image='$image' WHERE product\_id = $id LIMIT 1";

$r = mysqli\_query ($link, $q);

//If product successfully updated

if (mysqli\_affected\_rows($link) == 1) {

echo '<p class="text-center" style="color:green;">The product has been edited.</p>';

//If error occurred

} else {

echo '<p class="error text-center">The product could not be edited due to a system error.</p>';

}

} else { //Output errors

echo '<p class="error text-center">The following error(s) occurred:<br />';

foreach ($errors as $msg) { // Print each error.

echo " - $msg<br>\n";

}

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

}

}

//Query for products

$query = "SELECT \* FROM `storefront`.`entity\_product` AS `entity\_product` WHERE product\_id = '$id'";

$rs = mysqli\_query($link, $query);

//Query for product types

$queryType = "SELECT \* FROM `storefront`.`enum\_product\_type` AS `enum\_product\_type`";

$rsType = mysqli\_query($link, $queryType);

$numType = mysqli\_num\_rows($rsType); //Total number of product types

//If product ID chosen is valid

if (mysqli\_num\_rows($rs) == 1) {

//Get product information:

$row = mysqli\_fetch\_array($rs, MYSQLI\_NUM);

//Create form

echo '<div class="form">';

echo '<form action="edit\_product.php?id=' . $id . '" method="post">

<p>Product Name: <input type="text" name="product\_name" value="' . $row[1] . '"></p>

<p>Description: <input type="text" name="description" value="' . $row[2] . '"></p>

<p>Type: <select name="type">';

//Select box for product type

for ($i=0; $i<$numType; $i++) {

mysqli\_data\_seek($rsType, $i);

$rowType = $rsType->fetch\_assoc();

//Output product types as a drop down list, default select the original product type

if ($row[3] == $rowType['id']) {

echo '<option selected="' . $rowType['product\_type'] . '" value="' . ($i+1) . '">' . $rowType['product\_type'] . '</option>';

} else {

echo '<option value="' . ($i+1) . '">' . $rowType['product\_type'] . '</option>';

}

}

echo '</select>

<p>Color: <input type="text" name="color" value="' . $row[4] . '"> </p>

<p>Price: <input type="text" name="price" value="' . $row[5] . '"> </p>

<p>Image: <input type="text" name="image" value="' . $row[6] . '"> </p>

<p><input class="center" type="submit" name="submit" value="Update"></p>

<input type="hidden" name="id" value="' . $id . '" />

</form>';

echo '</div>';

echo '<div class="text-center">

<a href="inventory.php" class="btn btn-secondary">Go back to Inventory</a>

</div>';

echo '<span class="error"></span>';

}

else { //If product ID is not valid

echo '<h4 class="error text-center">This page has been accessed in error.</h4>';

}

//Product variant division

echo '<div class="page-header" style="margin-top:5%;"><h1><b>Product Variants</b></h1></div>';

echo "<div class='text-center' style='margin:5% 0%;'>";

echo '<a href="add\_product\_variant.php?id=' . $id . '" class="btn btn-primary">Add product variant</a><br><br>';

$query2 = "SELECT `entity\_product`.`product\_id`, `entity\_product\_variant`.`variant\_id`, `entity\_product\_variant`.`variant\_quantity`, `enum\_size`.`size`, `enum\_size`.`size\_id` FROM `storefront`.`entity\_product\_variant` AS `entity\_product\_variant`, `storefront`.`enum\_size` AS `enum\_size`, `storefront`.`entity\_product` AS `entity\_product`, `storefront`.`enum\_product\_type` AS `enum\_product\_type`, `storefront`.`xref\_product\_variant\_product` AS `xref\_product\_variant\_product` WHERE `entity\_product\_variant`.`variant\_size` = `enum\_size`.`size\_id` AND `entity\_product`.`type` = `enum\_product\_type`.`id` AND `xref\_product\_variant\_product`.`product\_id` = `entity\_product`.`product\_id` AND `xref\_product\_variant\_product`.`product\_variant\_id` = `entity\_product\_variant`.`variant\_id` AND `entity\_product`.`product\_id` = $id ORDER BY `enum\_size`.`size\_id` ASC";

$rs2 = mysqli\_query($link, $query2);

if (mysqli\_num\_rows($rs2) > 0) {

//Create table of variants

echo "<table class='tcenter' style='width:30%'>";

echo "<tr><th width=10%>" . 'Variant ID' . "</th>";

echo "<th width=10%>" . 'Size' . "</th>";

echo "<th width=10%>" . 'Quantity' . "</th>";

echo "<th width=7%></th>";

echo "<th width=7%></th></tr>";

while($re = mysqli\_fetch\_array($rs2, MYSQLI\_BOTH)) {

echo "<tr><td>" . $re['variant\_id'] . "</td>";

echo "<td>" . $re['size'] . "</td>";

echo "<td>" . $re['variant\_quantity'] . "</td>";

echo "<td class='edit'><a href='edit\_product\_variant.php?id\_1=" . $id . "&id\_2=" . $re['variant\_id'] . "'>Edit</a></td>";

echo "<td class='edit'><a href='delete\_product\_variant.php?id\_1=" . $id . "&id\_2=" . $re['variant\_id'] . "'>Delete</a></td></tr>";

}

echo "</table>";

echo "</div>";

} else {

echo '<p class="text-center">No variant found</p>';

}

mysqli\_close($link);

?>

</body>

</html>

**edit\_product\_variant.php**

<?php

$page\_title = 'Edit Product Variant';

include ('../includes/header.php');

require\_once "../config.php";

echo '<div class="page-header"><h2><b>Edit Product Variant</b></h2></div>';

//Check admin status

if (!isset($\_SESSION['admin']) || $\_SESSION['admin'] !== true) {

echo '<h4 class="error text-center">Error: Access denied</h4>';

exit;

}

//Check for a valid IDs through GET or POST

if ( isset($\_GET['id\_1']) && is\_numeric($\_GET['id\_1']) && isset($\_GET['id\_2']) && is\_numeric($\_GET['id\_2']) ) {

$id1 = $\_GET["id\_1"];

$id2 = $\_GET["id\_2"];

} elseif ( isset($\_POST['id\_1']) && is\_numeric($\_POST['id\_1']) && isset($\_POST['id\_2']) && is\_numeric($\_POST['id\_2']) ) {

$id1 = $\_POST["id\_1"];

$id2 = $\_POST["id\_2"];

} else {

echo '<h4 class="error text-center">Error: Product variant not found</h4>';

exit;

}

//Check if form has been submitted

if ($\_SERVER['REQUEST\_METHOD'] == 'POST') {

//Check product quantity

if (!empty($\_POST['quantity'])) {

$qty = mysqli\_real\_escape\_string($link, trim($\_POST['quantity']));

}

//Make the query

$query = "UPDATE `entity\_product\_variant` SET `variant\_quantity` = $qty WHERE `variant\_id` = $id2";

mysqli\_query($link, $query);

//If product variant successfully updated

if (mysqli\_affected\_rows($link) == 1) {

echo '<p class="text-center" style="color:green;">The product variant has been edited.</p>';

//If error occurred

} else {

echo '<p class="error text-center">The product variant could not be edited due to a system error.</p>';

}

}

$sql = "SELECT `entity\_product`.`product\_id`, `entity\_product\_variant`.`variant\_id`, `entity\_product`.`product\_name`, `enum\_size`.`size`, `entity\_product\_variant`.`variant\_quantity` FROM `storefront`.`entity\_product` AS `entity\_product`, `storefront`.`enum\_product\_type` AS `enum\_product\_type`, `storefront`.`entity\_product\_variant` AS `entity\_product\_variant`, `storefront`.`enum\_size` AS `enum\_size`, `storefront`.`xref\_product\_variant\_product` AS `xref\_product\_variant\_product` WHERE `entity\_product`.`type` = `enum\_product\_type`.`id` AND `entity\_product\_variant`.`variant\_size` = `enum\_size`.`size\_id` AND `xref\_product\_variant\_product`.`product\_id` = `entity\_product`.`product\_id` AND `xref\_product\_variant\_product`.`product\_variant\_id` = `entity\_product\_variant`.`variant\_id` AND `entity\_product`.`product\_id` = $id1 AND `entity\_product\_variant`.`variant\_id` = $id2";

$rs = mysqli\_query($link, $sql);

if (mysqli\_num\_rows($rs) == 1) {

//Get product information:

$row = mysqli\_fetch\_array ($rs, MYSQLI\_NUM);

//Display the record being deleted

echo "<div class='text-center'>";

echo "<h3>Product name: $row[2]</h3>

<h3>Size: $row[3]</h3>

<h3>Current Quantity: $row[4]</h3>";

echo "</div>";

}

?>

<div class="form">

<form action="edit\_product\_variant.php" method="post">

<p>Quantity: <input type="number" style="width:50px;" min="1" name="quantity" value="<?php echo $row[4]; ?>"></p>

<input type="submit" class="center" name="submit" value="Update" />

<input type="hidden" name="id\_1" value="<?php echo $id1; ?>">

<input type="hidden" name="id\_2" value="<?php echo $id2; ?>">

</form>

</div>

<div class="text-center">

<a href="inventory.php" class="btn btn-secondary">Go back to Inventory</a>

</div>

</body>

</html>

**edit\_user.php**

<?php

$page\_title = 'Edit User';

include ('../includes/header.php');

require ('../config.php');

echo '<div class="page-header"><h2><b>Edit User</b></h2></div>';

//Check admin status

if (!isset($\_SESSION['admin']) || $\_SESSION['admin'] !== true) {

echo '<h4 class="error text-center">Error: Access denied</h4>';

exit;

}

//Check for a valid user ID, through GET or POST

if ( (isset($\_GET['id'])) && (is\_numeric($\_GET['id'])) ) {

$id = $\_GET['id'];

} elseif ( (isset($\_POST['id'])) && (is\_numeric($\_POST['id'])) ) {

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

} else { //No valid ID, kill the script

echo '<h4 class="error text-center">Error: User not found</h4>';

exit;

}

//Check if the form has been submitted:

if ($\_SERVER['REQUEST\_METHOD'] == 'POST') {

//Array to hold errors

$errors = array();

//Check for a first name

if (empty($\_POST['first\_name'])) {

$errors[] = 'You forgot to enter first name.';

} else {

$fn = mysqli\_real\_escape\_string($link, trim($\_POST['first\_name']));

}

//Check for a last name

if (empty($\_POST['last\_name'])) {

$errors[] = 'You forgot to enter your last name.';

} else {

$ln = mysqli\_real\_escape\_string($link, trim($\_POST['last\_name']));

}

//Check for an email address

if (empty($\_POST['email'])) {

$errors[] = 'You forgot to enter your email address.';

} else {

$e = mysqli\_real\_escape\_string($link, trim($\_POST['email']));

}

if (empty($errors)) { //No errors found

//Test for unique email address in database

$q = "SELECT user\_id FROM entity\_user WHERE email = '$e' AND user\_id != $id";

$r = mysqli\_query($link, $q);

if (mysqli\_num\_rows($r) == 0) {

//Make query

$q = "UPDATE entity\_user SET first\_name='$fn', last\_name='$ln', email='$e' WHERE user\_id=$id LIMIT 1";

$r = mysqli\_query($link, $q);

if (mysqli\_affected\_rows($link) == 1) { //Successful edit of user details

echo '<p class="text-center">The user has been edited.</p>';

} else { //Not successful

echo '<div class="text-center"><p class="error">The user could not be edited due to a system error. We apologize for any inconvenience.</p>'; // Public message.

echo '<p>' . mysqli\_error($link) . '<br />Query: ' . $q . '</p></div>'; // Debugging message.

}

} else { //Already registered

echo '<p class="error text-center">The email address has already been registered.</p>';

}

} else { //Report the errors

echo '<div class="text-center"><p class="error">The following error(s) occurred:<br />';

foreach ($errors as $msg) { // Print each error.

echo " - $msg<br />\n";

}

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

}

}

//Retrieve the users information

$q = "SELECT email, first\_name, last\_name FROM entity\_user WHERE user\_id = $id";

$r = mysqli\_query($link, $q);

//Show form

if (mysqli\_num\_rows($r) == 1) {

//Get the user information

$row = mysqli\_fetch\_array($r, MYSQLI\_NUM);

//Create form

echo '<div class="form">

<form action="edit\_user.php" method="post">

<p>Email Address: <input type="text" name="email" value="' . $row[0] . '" /></p>

<p>First Name: <input type="text" name="first\_name" value="' . $row[1] . '" /></p>

<p>Last Name: <input type="text" name="last\_name" value="' . $row[2] . '" /></p>

<p><input type="submit" class="center" name="submit" value="Submit" /></p>

<input type="hidden" name="id" value="' . $id . '" />

</form>';

echo '<div class="text-center">

<a href="view\_user.php" class="btn btn-secondary">Go back to Users</a>

</div>';

} else { //Not a valid user ID

echo '<p class="error text-center">This page has been accessed in error.</p>';

echo '<div class="text-center">

<a href="view\_user.php" class="btn btn-secondary">Go back to Users</a>

</div>';

}

mysqli\_close($link);

?>

**inventory.php**

<?php

$page\_title = 'Manage Inventory';

include ('../includes/header.php');

require\_once "../config.php";

echo '<div class="page-header"><h2><b>Inventory Manager</b></h2></div>';

if (!isset($\_SESSION['admin']) || $\_SESSION['admin'] !== true) {

echo '<h4 class="error text-center">Error: Access denied</h4>';

exit;

}

//Number of records to show per page

$display = 7;

//Determine how many pages there are

if (isset($\_GET['p']) && is\_numeric($\_GET['p'])) { // Already been determined.

$pages = $\_GET['p'];

} else { //Need to determine pages

//Count number of records

$q = "SELECT COUNT(product\_id) FROM entity\_product";

$r = mysqli\_query ($link, $q);

$row = mysqli\_fetch\_array($r, MYSQLI\_NUM);

$records = $row[0];

//Calculate number of pages

if ($records > $display) { //More than 1 page

$pages = ceil ($records/$display);

} else {

$pages = 1;

}

}

//Determine where in the database to start returning results

if (isset($\_GET['s']) && is\_numeric($\_GET['s'])) {

$start = $\_GET['s'];

} else {

$start = 0;

}

//Default is by registration date

$sort = (isset($\_GET['sort'])) ? $\_GET['sort'] : 'pid';

//Determine sort

switch ($sort) {

case 'pid':

$order\_by = 'product\_id ASC';

break;

case 'name':

$order\_by = 'product\_name ASC';

break;

case 'type':

$order\_by = 'product\_type ASC';

break;

case 'col':

$order\_by = 'product\_color ASC';

break;

case 'p':

$order\_by = 'product\_price ASC';

break;

default:

$order\_by = 'product\_id ASC';

$sort = 'pid';

break;

}

//Query products with page limit

$sql = "SELECT `entity\_product`.\*, `enum\_product\_type`.`product\_type` FROM `storefront`.`entity\_product` AS `entity\_product`, `storefront`.`enum\_product\_type` AS `enum\_product\_type` WHERE `entity\_product`.`type` = `enum\_product\_type`.`id` ORDER BY $order\_by LIMIT $start, $display";

$rs = mysqli\_query($link,$sql);

//Output information

echo "<div class='text-center'>";

echo '<a href="add\_product.php" class="btn btn-primary">Add product</a><br><br>'; //Add product button

//Output table of inventory products

echo '<table class="tcenter">

<tr>

<th>Image</th>

<th width=10%><a href="inventory.php?sort=pid">Product ID</a></th>

<th width=15%><a href="inventory.php?sort=name">Name</a></th>

<th width=15%>Description</th>

<th><a href="inventory.php?sort=type">Type</a></th>

<th><a href="inventory.php?sort=col">Color</a></th>

<th><a href="inventory.php?sort=p">Price</a></th>

<th width=7%></th>

<th width=7%></th>

</tr>';

while($re = mysqli\_fetch\_array($rs, MYSQLI\_BOTH)) {

echo "<tr><td><img height='100px;' width='300px;' src='/Storefront/img/{$re['image']}'</td>";

echo "<td>" . $re['product\_id'] . "</td>";

echo "<td>" . $re['product\_name'] . "</td>";

echo "<td>" . $re['description'] . "</td>";

echo "<td>" . $re['product\_type'] . "</td>";

echo "<td>" . $re['product\_color'] . "</td>";

echo "<td>$" . $re['product\_price'] . "</td>";

echo "<td><a href='edit\_product.php?id=" . $re['product\_id'] . "'>Edit</a></td>"; //Edit product link

echo "<td><a href='delete\_product.php?id=" . $re['product\_id'] . "'>Delete</a></td></tr>"; //Delete product link

}

echo "</table>";

echo "</div>";

mysqli\_close($link);

//Pagination

if ($pages > 1) {

echo '<div class="text-center">';

echo '<br /><p>';

$current\_page = ($start/$display) + 1;

//If it's not the first page, make a previous button:

if ($current\_page != 1) {

echo '<a href="inventory.php?s=' . ($start - $display) . '&p=' . $pages . '&sort=' . $sort . '">Previous</a> ';

}

//Make all the numbered pages:

for ($i = 1; $i <= $pages; $i++) {

if ($i != $current\_page) {

echo '<a href="inventory.php?s=' . (($display \* ($i - 1))) . '&p=' . $pages . '&sort=' . $sort . '">' . $i . '</a> ';

} else {

echo $i . ' ';

}

}

//If it's not the last page, make a next button:

if ($current\_page != $pages) {

echo '<a href="inventory.php?s=' . ($start + $display) . '&p=' . $pages . '&sort=' . $sort . '">Next</a>';

}

echo '</p>';

echo '</div>';

}

?>

</body>

</html>

**register\_admin.php**

<?php

//Changed username -> email

$page\_title = 'Register Admin';

include ('../includes/header.php');

require\_once "../config.php";

//Define variables and initialize with empty values

$username = $password = $confirm\_password = "";

$username\_err = $password\_err = $confirm\_password\_err = "";

//Processing form data when form is submitted

if ($\_SERVER["REQUEST\_METHOD"] == "POST") {

// Validate username

if (empty(trim($\_POST["username"]))) {

$username\_err = "Please enter a username.";

} else {

//Prepare a select statement

$sql = "SELECT email FROM entity\_user WHERE email = ?";

if ($stmt = mysqli\_prepare($link, $sql)) {

//Bind variables to the prepared statement as parameters

mysqli\_stmt\_bind\_param($stmt, "s", $param\_username);

//Set parameters

$param\_username = trim($\_POST["username"]);

//Attempt to execute the prepared statement

if (mysqli\_stmt\_execute($stmt)) {

mysqli\_stmt\_store\_result($stmt); //Store result

if (mysqli\_stmt\_num\_rows($stmt) == 1) {

$username\_err = "This username is already taken.";

} else {

$username = trim($\_POST["username"]);

}

} else {

echo "Oops! Something went wrong. Please try again later.";

}

// Close statement

mysqli\_stmt\_close($stmt);

}

}

// Validate password

if (empty(trim($\_POST["password"]))) {

$password\_err = "Please enter a password.";

} else {

$password = trim($\_POST["password"]);

}

//Validate confirm password

if (empty(trim($\_POST["confirm\_password"]))) {

$confirm\_password\_err = "Please confirm password.";

} else {

$confirm\_password = trim($\_POST["confirm\_password"]);

if(empty($password\_err) && ($password != $confirm\_password)) {

$confirm\_password\_err = "Password does not match.";

}

}

// Check input errors before inserting in database

if (empty($username\_err) && empty($password\_err) && empty($confirm\_password\_err)) {

$admin = 0; //Admin code

// Prepare an insert statement

$sql = "INSERT INTO entity\_user (email, password, role) VALUES (?, ?, $admin)";

if ($stmt = mysqli\_prepare($link, $sql)) {

// Bind variables to the prepared statement as parameters

mysqli\_stmt\_bind\_param($stmt, "ss", $param\_username, $param\_password);

// Set parameters

$param\_username = $username;

$param\_password = password\_hash($password, PASSWORD\_DEFAULT); // Creates a password hash

// Attempt to execute the prepared statement

if (mysqli\_stmt\_execute($stmt)) {

// Redirect to login page

header("location: /Storefront/login.php");

} else {

echo "Something went wrong. Please try again later.";

}

// Close statement

mysqli\_stmt\_close($stmt);

}

}

// Close connection

mysqli\_close($link);

}

?>

<div id="accountForm">

<form action="<?php echo htmlspecialchars($\_SERVER["PHP\_SELF"]); ?>" method="post">

<div class="container">

<h2>Register Admin</h2>

<p>Please enter the following information to create an account</p>

<hr>

<div class="form-group <?php echo (!empty($username\_err)) ? 'has-error' : ''; ?>">

<label>Username</label>

<input type="text" name="username" class="form-control" value="<?php echo $username; ?>" placeholder="Enter username here">

<span class="help-block"><?php echo $username\_err; ?></span>

</div>

<div class="form-group <?php echo (!empty($password\_err)) ? 'has-error' : ''; ?>">

<label>Password</label>

<input type="password" name="password" class="form-control" value="<?php echo $password; ?>" placeholder="Enter password here">

<span class="help-block"><?php echo $password\_err; ?></span>

</div>

<div class="form-group <?php echo (!empty($confirm\_password\_err)) ? 'has-error' : ''; ?>">

<label>Confirm Password</label>

<input type="password" name="confirm\_password" class="form-control" value="<?php echo $confirm\_password; ?>" placeholder="Repeat password here">

<span class="help-block"><?php echo $confirm\_password\_err; ?></span>

</div>

<div class="form-group">

<br><button type="submit">Register</button>

</div>

</div>

</form>

</div>

</body>

</html>

**view\_user.php**

<?php

$page\_title = 'View Users';

include ('../includes/header.php');

require ('../config.php'); //Connect DB

echo '<div class="page-header"><h2><b>User List</b></h2></div>';

//Check admin status

if (!isset($\_SESSION['admin']) || $\_SESSION['admin'] !== true) {

echo '<h4 class="error text-center">Error: Access denied</h4>';

exit;

}

//Number of records to show per page

$display = 5;

//Determine how many pages there are

if (isset($\_GET['p']) && is\_numeric($\_GET['p'])) { // Already been determined.

$pages = $\_GET['p'];

} else { //Need to determine pages

//Count number of records

$q = "SELECT COUNT(user\_id) FROM entity\_user";

$r = mysqli\_query ($link, $q);

$row = mysqli\_fetch\_array($r, MYSQLI\_NUM);

$records = $row[0];

//Calculate number of pages

if ($records > $display) { //More than 1 page

$pages = ceil ($records/$display);

} else {

$pages = 1;

}

}

//Determine where in the database to start returning results

if (isset($\_GET['s']) && is\_numeric($\_GET['s'])) {

$start = $\_GET['s'];

} else {

$start = 0;

}

//Default is by registration date

$sort = (isset($\_GET['sort'])) ? $\_GET['sort'] : 'rd';

//Determine sort

switch ($sort) {

case 'e':

$order\_by = 'email ASC';

break;

case 'fn':

$order\_by = 'first\_name ASC';

break;

case 'ln':

$order\_by = 'last\_name ASC';

break;

case 'rd':

$order\_by = 'registration\_date ASC';

break;

default:

$order\_by = 'registration\_date ASC';

$sort = 'rd';

break;

}

//Query

$q = "SELECT `user\_id`, `email`, `first\_name`, `last\_name`, `registration\_date`, `role` FROM `storefront`.`entity\_user` AS `entity\_user` WHERE `role` = 1 ORDER BY $order\_by LIMIT $start, $display";

$r = mysqli\_query ($link, $q); //Run the query

//Table header

echo '<table align="center" cellspacing="0" cellpadding="5" width="75%">

<tr>

<td width="7%"></td>

<td width="7%"></td>

<td width="30%"><b><a href="view\_user.php?sort=e">Email</a></b></td>

<td><b><a href="view\_user.php?sort=fn">First Name</a></b></td>

<td><b><a href="view\_user.php?sort=ln">Last Name</a></b></td>

<td width="30%"><b><a href="view\_user.php?sort=rd">Date Registered</a></b></td>

</tr>';

//Fetch and print all records

while ($row = mysqli\_fetch\_array($r, MYSQLI\_ASSOC)) {

echo '<tr>

<td><a href="edit\_user.php?id=' . $row['user\_id'] . '">Edit</a></td>

<td><a href="delete\_user.php?id=' . $row['user\_id'] . '">Delete</a></td>

<td>' . $row['email'] . '</td>

<td>' . $row['first\_name'] . '</td>

<td>' . $row['last\_name'] . '</td>

<td>' . $row['registration\_date'] . '</td>

</tr>';

}

echo '</table>';

mysqli\_free\_result($r);

mysqli\_close($link);

//Pagination

if ($pages > 1) {

echo '<div class="text-center">';

echo '<br /><p>';

$current\_page = ($start/$display) + 1;

//If it's not the first page, make a previous button:

if ($current\_page != 1) {

echo '<a href="view\_user.php?s=' . ($start - $display) . '&p=' . $pages . '&sort=' . $sort . '">Previous</a> ';

}

//Make all the numbered pages:

for ($i = 1; $i <= $pages; $i++) {

if ($i != $current\_page) {

echo '<a href="view\_user.php?s=' . (($display \* ($i - 1))) . '&p=' . $pages . '&sort=' . $sort . '">' . $i . '</a> ';

} else {

echo $i . ' ';

}

}

//If it's not the last page, make a next button:

if ($current\_page != $pages) {

echo '<a href="view\_user.php?s=' . ($start + $display) . '&p=' . $pages . '&sort=' . $sort . '">Next</a>';

}

echo '</p>';

echo '</div>';

}

?>

**header.php**

<?php

session\_start();

?>

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title><?php echo $page\_title; ?></title>

<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.0/css/bootstrap.min.css">

<link href="https://fonts.googleapis.com/css?family=Roboto+Slab" rel="stylesheet">

<link href="/Storefront/stylesheet.css" rel="stylesheet">

<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.4.0/jquery.min.js"></script>

</head>

<body>

<nav class="navbar navbar-default">

<div class="container-fluid">

<a class="navbar-brand" href="/Storefront/home.php">

<img id="logo" src="/Storefront/img/logo.png" style="position:relative; top:-15px;">

</a>

<ul class="nav navbar-nav navbar-right">

<?php

if (isset($\_SESSION['loggedin'])) {

if (!isset($\_SESSION['admin']) || $\_SESSION['admin'] !== true) {

echo "<li><a href='/Storefront/account.php'><span class='glyphicon glyphicon-user'></span> Account</a></li>";

} else {

echo "<li><a href='/Storefront/admin/admin.php'><span class='glyphicon glyphicon-user'></span> Admin</a></li>";

}

echo "<li><a href='/Storefront/logout.php'><span class='glyphicon glyphicon-log-out'></span> Log Out</a></li>";

} else {

echo "<li><a href='/Storefront/register.php'><span class='glyphicon glyphicon-user'></span> Register</a></li>";

echo "<li><a href='/Storefront/login.php'><span class='glyphicon glyphicon-log-in'></span> Log In</a></li>";

}

?>

<li><a href="/Storefront/view\_cart.php"><span class="glyphicon glyphicon-shopping-cart"></span> Cart<span class="badge badge-light"><?php echo (isset($\_SESSION['cart'])) ? count($\_SESSION['cart']) : 0; ?></span></a></li>

</ul>

</div>

</nav>

**footer.html**

<!DOCTYPE html>

<div class="footer">

<p>Contact: <a href="mailto:bkwon01@student.rccd.edu">bkwon1@student.rccd.edu</a></p> </div> </body>

</html>

**account.php**

<?php

$page\_title = 'Account';

include ('./includes/header.php');

require\_once "./config.php";

if(!isset($\_SESSION["loggedin"]) && $\_SESSION["loggedin"] !== true) {

header("location: login.php");

exit;

}

?>

<div class="page-header">

<h1>Welcome, <b><?php echo htmlspecialchars($\_SESSION["firstname"]); ?></b></h1>

</div>

<div class="text-center">

<a href="view\_order.php" style="width:150px;" class="btn btn-primary">View Orders</a><br><br>

<div class="settings">

<h3><span class="glyphicon glyphicon-cog"></span> Settings</h3>

<a href="/Storefront/reset\_password.php" class="btn btn-warning">Reset password</a>

</div>

</div>

**add\_cart.php**

<?php

$page\_title = 'Cart';

include ('includes/header.php');

require\_once "config.php";

//Decode object

$obj = json\_decode($\_COOKIE["product"]);

//Set variables

$varID = $obj->varID; //Product ID

$qty = $obj->qty; //Quantity

//Check if the cart already contains the same item

if (isset($\_SESSION['cart'][$varID])) {

//Add new quantity

$\_SESSION['cart'][$varID]['quantity'] += $qty;

echo '<p class="text-center">Shopping cart has been updated.</p>';

header("location: view\_cart.php");

} else { //New product

//Query for price of product variant

$q = "SELECT `entity\_product\_variant`.`variant\_id`, `entity\_product`.`product\_price` FROM `storefront`.`xref\_product\_variant\_product` AS `xref\_product\_variant\_product`, `storefront`.`entity\_product` AS `entity\_product`, `storefront`.`entity\_product\_variant` AS `entity\_product\_variant` WHERE `xref\_product\_variant\_product`.`product\_id` = `entity\_product`.`product\_id` AND `xref\_product\_variant\_product`.`product\_variant\_id` = `entity\_product\_variant`.`variant\_id` AND `entity\_product\_variant`.`variant\_id` = '$varID'";

$r = mysqli\_query($link, $q);

//Get price

if (mysqli\_num\_rows($r) == 1) {

$row = $r->fetch\_assoc();

$price = $row['product\_price'];

}

//Add to cart, utilize session

$\_SESSION['cart'][$varID] = array('quantity' => $qty, 'price' => $price);

header("location: view\_cart.php");

}

**checkout.php**

<?php

$page\_title = 'Checkout';

include ('includes/header.php');

require\_once "config.php";

//First, check if user is logged in. If not, redirect

if (!isset($\_SESSION['loggedin']) && $\_SESSION['loggedin'] !== true) {

header("location: login.php");

exit;

} elseif (!isset($\_SESSION['order\_total']) || !isset($\_SESSION['id'])) {

echo '<p class="error text-center">Access denied</p>';

exit;

} else {

$userID = $\_SESSION['id']; //Get user ID

$total = $\_SESSION['order\_total']; //Get total price

}

//Insert into order database

$q = "INSERT INTO entity\_order (order\_total) VALUES ($total)";

$r = mysqli\_query($link, $q);

$orderID = $link->insert\_id; //Store primary key of order created

if (mysqli\_affected\_rows($link) == 1) {

//Insert into xref\_user\_order - connect user and order

$q2 = "INSERT INTO xref\_user\_order (order\_id, user\_id) VALUES ($orderID, $userID)";

$r2 = mysqli\_query($link, $q2);

if (mysqli\_affected\_rows($link) == 1) {

foreach ($\_SESSION['cart'] as $varID => $item) {

$qty = $item['quantity']; //Get quantity

$price = $item['price']; //Get price

//Insert individual items of the order into database

$q3 = "INSERT INTO entity\_order\_item (order\_item\_quantity, order\_item\_price) VALUES ($qty, $price)";

$r3 = mysqli\_query($link, $q3);

$last\_id = $link->insert\_id; //Last entered PrimaryID of entity order\_item from previous query

//Insert xref\_order\_item\_product\_variant - connect order item and product variant

$q4 = "INSERT INTO xref\_order\_item\_product\_variant (order\_item\_id, product\_variant\_id) VALUES ($last\_id, $varID)";

$r4 = mysqli\_query($link, $q4);

$last\_id = $link->insert\_id; //Last entered primary ID of order item

//Insert into xref\_order\_order\_item - connect order and ordered items

$q5 = "INSERT INTO xref\_order\_order\_item (order\_id, order\_item\_id) VALUES ($orderID, $last\_id)";

$r5 = mysqli\_query($link, $q5);

}

//Make sure success

unset($\_SESSION['cart']); //Clear cart

//Output message

echo '<div class="page-header"><h2><b>Order Success</b></h2></div>

<div class="text-center">

<h4 style="padding-bottom:100px;">Thank you for your order!<br>A confirmation email will be delivered to you shortly.</h4>

<a href="home.php" style="width:200px;" class="btn btn-success">Continue Shopping</a>

</div>';

}

} else {

echo '<p class="text-center">Your order could not be processed due to a system error. We apologize for any inconvenience. Please try again later</p>';

}

mysqli\_close($link);

?>

**config.php**

<?php

/\* Database credentials. Assuming you are running MySQL

server with default setting (user 'root' with no password) \*/

define('DB\_SERVER', 'localhost');

define('DB\_USERNAME', 'root');

define('DB\_PASSWORD', '');

define('DB\_NAME', 'storefront');

/\* Attempt to connect to MySQL database \*/

$link = mysqli\_connect(DB\_SERVER, DB\_USERNAME, DB\_PASSWORD, DB\_NAME);

// Check connection

if ($link === false){

die("ERROR: Could not connect. " . mysqli\_connect\_error());

}

?>

**home.php**

<?php

$page\_title = 'Home';

include ('includes/header.php');

require\_once "config.php";

//Number of records to show per page

$display = 6;

//Determine how many pages there are

if (isset($\_GET['p']) && is\_numeric($\_GET['p'])) { //Already on a page

$pages = $\_GET['p'];

} else { //Need to determine pages

//Count number of records

if (isset($\_GET['cat'])) {

$cat = $\_GET['cat'];

$q = "SELECT COUNT(product\_id) FROM entity\_product WHERE type = '$cat'";

} else {

$q = "SELECT COUNT(product\_id) FROM entity\_product";

}

$r = mysqli\_query ($link, $q);

$row = mysqli\_fetch\_array($r, MYSQLI\_NUM);

$records = $row[0];

//Calculate number of pages

if ($records > $display) { //More than 1 page

$pages = ceil ($records/$display);

} else {

$pages = 1;

}

}

//Determine where in the database to start returning results

if (isset($\_GET['s']) && is\_numeric($\_GET['s'])) {

$start = $\_GET['s'];

} else {

$start = 0;

}

//Determine the sort

//Default is by registration date

$sort = (isset($\_GET['sort'])) ? $\_GET['sort'] : 'rd';

// Determine the sorting order:

switch ($sort) {

case 'plo':

$order\_by = 'product\_price ASC';

break;

case 'phi':

$order\_by = 'product\_price DESC';

break;

default:

$order\_by = 'type ASC';

$sort = 'type';

break;

}

?>

<div class="container-fluid home">

<div class="jumbotron">

<a href="home.php"><img class="center img-responsive" src="./img/banner.png"></a>

</div>

<div class="col-sm-2 sidenav well">

<h4>Categories</h4>

<ul class="nav nav-stacked">

<li><a style="color:black;" href="home.php">All</a></li>

<?php

//Get product type categories

$qCat = "SELECT \* FROM `storefront`.`enum\_product\_type` AS `enum\_product\_type`";

$rsCat = mysqli\_query($link, $qCat);

while($re = mysqli\_fetch\_array($rsCat, MYSQLI\_BOTH)) {

echo '<li><a style="color: black;" href="home.php?cat=' . $re['id'] . '">' . $re['product\_type'] . '</a></li>';

}

?>

</ul>

<br>

<h4>Sort by</h4>

<ul class="nav nav-stacked">

<?php

if (isset($\_GET['cat'])) { //Category and price

echo '<li><a style="color:black;" href="home.php?sort=plo&cat=' . $\_GET['cat'] . '">Price low to high</a></li>';

echo '<li><a style="color:black;" href="home.php?sort=phi&cat=' . $\_GET['cat'] . '">Price high to low</a></li>';

} else { //Only price

echo '<li><a style="color:black;" href="home.php?sort=plo">Price low to high</a></li>';

echo '<li><a style="color:black;" href="home.php?sort=phi">Price high to low </a></li>';

}

?>

</ul>

</div>

<div class="col-sm-10">

<?php

if (isset($\_GET['cat'])) {

$cat = $\_GET['cat'];

$query = "SELECT `product\_id`, `product\_name`, `product\_price`, `image`, `type` FROM `storefront`.`entity\_product` AS `entity\_product` WHERE `type` = '$cat' ORDER BY $order\_by LIMIT $start, $display";

} else {

$query = "SELECT `product\_id`, `product\_name`, `product\_price`, `image` FROM `storefront`.`entity\_product` AS `entity\_product` ORDER BY $order\_by LIMIT $start, $display";

}

$rs = mysqli\_query($link, $query);

$counter = 0;

$itemPerRow = 3;

if (mysqli\_num\_rows($rs) == 0) {

echo '<p style="text-align:center; padding-top:100px;">No items found. Check again later.</p>';

} else {

echo '<div class="row">';

while ($re = mysqli\_fetch\_array($rs,MYSQLI\_BOTH)) {

if ($counter%$itemPerRow == 0) {

echo '</div><div class="row">';

}

echo '<div class="col-sm-4">';

echo '<div class="panel panel-default">';

echo '<div class="panel-body"><a href="product.php?id=' . $re['product\_id'] . '"><img src="./img/' . $re['image'] . '" class="img-responsive" style="width:100%" alt="Image"></div>';

echo '<div class="panel-footer text-center">';

echo '<p>' . $re['product\_name'] . '</p></a>';

echo '<p>$' . $re['product\_price'] . '</p>';

echo '</div>';

echo '</div>';

echo '</div>';

$counter++;

}

echo '</div>';

}

?>

</div>

</div>

<?php

//Pagination

if ($pages > 1) {

echo '<div class="text-center">';

echo '<br><p>';

$current\_page = ($start/$display) + 1;

//If it's not the first page, make a previous button

if ($current\_page != 1) {

echo '<a href="home.php?s=' . ($start - $display) . '&p=' . $pages . '&sort=' . $sort . '">Previous</a> ';

}

//Make all the numbered pages

for ($i = 1; $i <= $pages; $i++) {

if ($i != $current\_page) {

echo '<a href="home.php?s=' . (($display \* ($i - 1))) . '&p=' . $pages . '&sort=' . $sort . '">' . $i . '</a> ';

} else {

echo $i . ' ';

}

}

//If it's not the last page, make a next button

if ($current\_page != $pages) {

echo '<a href="home.php?s=' . ($start + $display) . '&p=' . $pages . '&sort=' . $sort . '">Next</a>';

}

echo '</p>';

echo '</div>';

}

include('includes/footer.html');

?>

**login.php**

<?php

$page\_title = 'Login';

include ('includes/header.php');

require\_once "config.php";

//Check if user is already logged in, if so, redirect to account page

if (isset($\_SESSION["loggedin"]) && $\_SESSION["loggedin"] === true) {

//Check if user is an admin or not

if (isset($\_SESSION["admin"]) && $\_SESSION["admin"] === true) {

header("location: /Storefront/admin/admin.php");

} else {

header("location: account.php");

}

exit;

}

//Define variables and initialize with empty values

$email = $password = "";

$email\_err = $password\_err = "";

// Processing form data when form is submitted

if ($\_SERVER["REQUEST\_METHOD"] == "POST") {

//Check if email is empty

if (empty(trim($\_POST["email"]))) {

$email\_err = "Please enter email.";

} else {

$email = trim($\_POST["email"]);

}

//Check if password is empty

if (empty(trim($\_POST["password"]))) {

$password\_err = "Please enter your password.";

} else {

$password = trim($\_POST["password"]);

}

//Validate credentials

if (empty($email\_err) && empty($password\_err)) {

// Prepare a select statement

$sql = "SELECT user\_id, email, password, role, first\_name FROM entity\_user WHERE email = ?";

if ($stmt = mysqli\_prepare($link, $sql)) {

//Bind variables to the prepared statement as parameters

mysqli\_stmt\_bind\_param($stmt, "s", $param\_email);

//Set parameters

$param\_email = $email;

//Attempt to execute the prepared statement

if (mysqli\_stmt\_execute($stmt)) {

//Store result

mysqli\_stmt\_store\_result($stmt);

//Check if email exists, if yes then verify password

if (mysqli\_stmt\_num\_rows($stmt) == 1) {

//Bind result variables

mysqli\_stmt\_bind\_result($stmt, $id, $email, $hashed\_password, $role, $fn);

if (mysqli\_stmt\_fetch($stmt)) {

if (password\_verify($password, $hashed\_password)) {

//Password is correct, so start a new session

session\_start();

//Store data in session variables

$\_SESSION["loggedin"] = true;

$\_SESSION["id"] = $id;

$\_SESSION["firstname"] = $fn;

if ($role == 0) { //If admin

$\_SESSION["admin"] = true;

$\_SESSION["firstname"] = "admin";

//Redirect to admin page

header("location: /Storefront/admin/admin.php");

} else { //If regular user

$\_SESSION["admin"] = false;

// Redirect user to welcome page

header("location: /Storefront/account.php");

}

} else {

// Display an error message if password is not valid

$password\_err = "The password you entered was not valid.";

}

}

} else {

// Display an error message if email doesn't exist

$email\_err = "No account found with that email.";

}

} else {

echo "Oops! Something went wrong. Please try again later.";

}

//Close statement

mysqli\_stmt\_close($stmt);

}

}

//Close connection

mysqli\_close($link);

}

?>

<div id="accountForm">

<form action="" method="post">

<div class="container">

<h2>Login</h2>

<hr>

<div class="form-group <?php echo (!empty($email\_err)) ? 'has-error' : ''; ?>" >

<label>Email</label>

<input type="text" name="email" class="form-control" value="<?php echo $email; ?>" placeholder="Enter Email">

<span class="help-block"><?php echo $email\_err; ?></span>

</div>

<div class="form-group <?php echo (!empty($password\_err)) ? 'has-error' : ''; ?>" >

<label>Password</label>

<input type="password" name="password" class="form-control" placeholder="Enter Password">

<span class="help-block"><?php echo $password\_err; ?></span>

</div>

<p>No account? <a href="./register.php">Register here.</a></p>

<div class="form-group" style="padding-top:25px">

<button type="submit">Login</button>

</div>

</div>

</form>

</div>

</body>

</html>

**logout.php**

<?php

//Initialize session

session\_start();

//Unset all session variables

$\_SESSION = array();

//Destroy session

session\_destroy();

//Redirect

header("location: home.php");

exit;

?>

**product.php**

<?php

$page\_title = 'View Product';

include ('includes/header.php');

require\_once "config.php";

if (isset($\_GET['id']) && isset($\_GET['vid'])) { //If variant ID is chosen

$id = $\_GET['id']; //ID

$vid = $\_GET['vid']; //Variant ID

} elseif (isset($\_GET['id'])) { //Regular product page

$id = $\_GET['id'];

} else {

echo '<h4 class="error text-center">Error: Product not found</h4>';

exit;

}

?>

<script>

class Product {

constructor(variant\_id, quantity, price) {

this.varID = variant\_id;

this.qty = quantity;

}

}

function addCart() {

//Quantity

var q = document.querySelector("#qty").value.trim();

if (q > 99 || q < 1) {

var err = document.getElementById("error");

err.style.display = "block"; //Toggle css display on

err.innerHTML = "Quantity must be within 1~99"; //Add & display error message

return;

}

//Size ID (from enum table)

var numBtn = document.querySelectorAll('.size-choose button').length;

for (var i=0; i<numBtn; i++) {

var x = document.getElementById("btn"+(i+1)).autofocus;

//If (x) console.log("focused"); else console.log("not focused");

if (x) {

var vid = document.getElementById("btn"+(i+1)).value; //Get variant ID

//Create product

var product = new Product(vid, parseInt(q));

var str = JSON.stringify(product);

document.cookie = "product=" + str;

window.location = "add\_cart.php"; //Go to cart

return;

}

}

var err = document.getElementById("error");

err.style.display = "block"; //Toggle css display on

err.innerHTML = "Please select a size option"; //Add & display error message

}

</script>

<?php

//Query the product

$q = "SELECT `entity\_product`.`product\_id`, `entity\_product\_variant`.`variant\_id`, `entity\_product`.`product\_name`, `entity\_product`.`description`, `enum\_product\_type`.`product\_type`, `entity\_product`.`product\_color`, `entity\_product`.`product\_price`, `entity\_product`.`image`, `entity\_product\_variant`.`variant\_size`, `enum\_size`.`size`, `enum\_size`.`size\_id` FROM `storefront`.`entity\_product` AS `entity\_product`, `storefront`.`enum\_product\_type` AS `enum\_product\_type`, `storefront`.`xref\_product\_variant\_product` AS `xref\_product\_variant\_product`, `storefront`.`entity\_product\_variant` AS `entity\_product\_variant`, `storefront`.`enum\_size` AS `enum\_size` WHERE `entity\_product`.`type` = `enum\_product\_type`.`id` AND `xref\_product\_variant\_product`.`product\_id` = `entity\_product`.`product\_id` AND `entity\_product\_variant`.`variant\_size` = `enum\_size`.`size\_id` AND `xref\_product\_variant\_product`.`product\_variant\_id` = `entity\_product\_variant`.`variant\_id` AND `entity\_product`.`product\_id` = $id ORDER BY `enum\_size`.`size\_id` ASC";

$r = mysqli\_query($link, $q);

$nSize = mysqli\_num\_rows($r); //Get number of sizes for the product

//If query successful, fetch first row in order to extract information

if (mysqli\_num\_rows($r) > 0) {

mysqli\_data\_seek($r, 0);

$row = $r->fetch\_assoc();

}

//Error

else {

echo '<div class="text-center">Product not available yet. Sorry for the inconvenience.</div>';

exit;

}

?>

<div class="product\_container">

<!--Product image, left column-->

<div class="left-column">

<img src="./img/<?php echo $row['image']; ?>" class="img-responsive center" alt="Image">

</div>

<!--Product details, right column-->

<div class="right-column">

<div class="product-description">

<h2> <?php echo $row['product\_name']; ?> </h2>

<h2> $<?php echo $row['product\_price']; ?> </h2><br>

<p> <?php echo $row['description']; ?> </p>

</div>

<div class="product-color">

<p>Color: <?php echo $row['product\_color']; ?> </p>

</div>

<div class="product-size">

<span>Size:</span>

<div class="size-choose">

<?php

for ($i=0; $i<$nSize; $i++) {

mysqli\_data\_seek($r, $i);

$rowSz = $r->fetch\_assoc();

if (isset($vid) && ($vid == $rowSz['variant\_id'])) {

echo '<button autofocus class="active" onclick="window.location.href=\'product.php?id=' . $id . '&vid=' . $rowSz['variant\_id'] . '\'" id="btn' . ($i+1) . '" name="size" value="' . $rowSz["variant\_id"] . '">' . $rowSz['size'] . '</button>';

} else {

echo '<button onclick="window.location.href=\'product.php?id=' . $id . '&vid=' . $rowSz['variant\_id'] . '\'" id="btn' . ($i+1) . '" name="size" value="' . $rowSz["variant\_id"] . '">' . $rowSz['size'] . '</button>';

}

}

?>

<input type="hidden" id="btnValue" value=""/>

</div>

</div>

<div class="product-quantity">

<p>Quantity: <input id="qty" type="number" name="qty" value="1" step="1" min ="1" max ="99" style="width:50px; text-align:right;"></p>

</div>

<?php echo '<button class="cart-btn" onclick="addCart()">Add to cart</button>'; ?>

<span id="error"></span>

</div>

</div>

</body>

</html>

**register.php**

<?php

$page\_title = 'Register';

include ('includes/header.php');

require\_once "config.php";

//Define variables and initialize with empty values

$email = $fn = $ln = $password = $confirm\_password = "";

$email\_err = $fn\_err = $ln\_err = $password\_err = $confirm\_password\_err = "";

//Email regex validation

function validate\_email($email) {

if ( !preg\_match("/^([a-zA-Z0-9])+([a-zA-Z0-9\.\_-])\*@([a-zA-Z0-9\_-])+([a-zA-Z0-9\.\_-]+)+$/", $email) ) {

return false;

}

return true;

}

//Password regex must be 6-20 characters including: a digit, a lower case char, a upper case char, a special symbol

function validate\_password($pass) {

if ( !preg\_match("/^((?=.\*\d)(?=.\*[a-z])(?=.\*[A-Z])(?=.\*[!@#$%^&\*]).{6,20})$/", $pass) ) {

return false;

}

return true;

}

//Processing form data when form is submitted

if ($\_SERVER["REQUEST\_METHOD"] == "POST") {

//Validate email

if (empty(trim($\_POST["email"]))) {

$email\_err = "Please enter an email address.";

} elseif (!validate\_email(trim($\_POST["email"]))) {

$email\_err = "Must be a valid email address";

} else {

//Prepare a select statement

$sql = "SELECT email FROM entity\_user WHERE email = ?";

if($stmt = mysqli\_prepare($link, $sql)){

//Bind variables to the prepared statement as parameters

mysqli\_stmt\_bind\_param($stmt, "s", $param\_email);

//Set parameters

$param\_email = trim($\_POST["email"]);

//Attempt to execute the prepared statement

if(mysqli\_stmt\_execute($stmt)){

//Store result

mysqli\_stmt\_store\_result($stmt);

if(mysqli\_stmt\_num\_rows($stmt) == 1){

$email\_err = "This email is already used.";

} else{

$email = trim($\_POST["email"]);

}

} else{

echo "Oops! Something went wrong. Please try again later.";

}

//Close statement

mysqli\_stmt\_close($stmt);

}

}

//Validate first name

if (empty(trim($\_POST["first\_name"]))) {

$fn\_err = "Please enter a first name.";

} else {

$fn = trim($\_POST["first\_name"]);

}

//Validate last name

if (empty(trim($\_POST["last\_name"]))) {

$ln\_err = "Please enter a last name.";

} else {

$ln = trim($\_POST["last\_name"]);

}

//Validate password

if (empty(trim($\_POST["password"]))) {

$password\_err = "Please enter a password.";

} elseif (strlen(trim($\_POST["password"])) < 6) {

$password\_err = "Password must have at least 6 characters.";

} elseif (!validate\_password(trim($\_POST["password"]))) {

$password\_err = "Password must have each of the following: digit, lowercase character, uppercase character, and a special symbol.";

} else {

$password = trim($\_POST["password"]);

}

//Validate confirm password

if (empty(trim($\_POST["confirm\_password"]))) {

$confirm\_password\_err = "Please confirm password.";

} else {

$confirm\_password = trim($\_POST["confirm\_password"]);

if (empty($password\_err) && ($password != $confirm\_password)) {

$confirm\_password\_err = "Password does not match.";

}

}

//Check input errors before inserting in database

if (empty($email\_err) && empty($password\_err) && empty($confirm\_password\_err) && empty($fn\_err) && empty($ln\_err)) {

$user = 1; //Regular user type code

// Prepare an insert statement

$sql = "INSERT INTO entity\_user (email, password, first\_name, last\_name, role) VALUES (?, ?, ?, ?, $user)";

if ($stmt = mysqli\_prepare($link, $sql)) {

//Bind variables to the prepared statement as parameters

mysqli\_stmt\_bind\_param($stmt, "ssss", $param\_email, $param\_password, $param\_fn, $param\_ln);

//Set parameters

$param\_email = $email;

$param\_password = password\_hash($password, PASSWORD\_DEFAULT); // Creates a password hash

$param\_fn = $fn;

$param\_ln = $ln;

//Attempt to execute the prepared statement

if (mysqli\_stmt\_execute($stmt)) {

//Redirect to login page

header("location: login.php");

} else {

echo "Something went wrong. Please try again later.";

}

//Close statement

mysqli\_stmt\_close($stmt);

}

}

//Close connection

mysqli\_close($link);

}

?>

<div id="accountForm">

<form action="<?php echo htmlspecialchars($\_SERVER["PHP\_SELF"]); ?>" method="post">

<div class="container">

<h2>Register</h2>

<p>Please enter the following information to create an account</p>

<hr>

<div class="form-group <?php echo (!empty($email\_err)) ? 'has-error' : ''; ?>">

<label>Email</label>

<input type="text" name="email" class="form-control" value="<?php echo $email; ?>" placeholder="Enter email here">

<span class="help-block"><?php echo $email\_err; ?></span>

</div>

<div class="form-group <?php echo (!empty($fn\_err)) ? 'has-error' : ''; ?>">

<label>First Name</label>

<input type="text" name="first\_name" class="form-control" value="<?php echo $fn; ?>" placeholder="Enter first name here">

<span class="help-block"><?php echo $fn\_err; ?></span>

</div>

<div class="form-group <?php echo (!empty($ln\_err)) ? 'has-error' : ''; ?>">

<label>Last Name</label>

<input type="text" name="last\_name" class="form-control" value="<?php echo $ln; ?>" placeholder="Enter last name here">

<span class="help-block"><?php echo $ln\_err; ?></span>

</div>

<div class="form-group <?php echo (!empty($password\_err)) ? 'has-error' : ''; ?>">

<label>Password</label>

<input type="password" name="password" class="form-control" value="<?php echo $password; ?>" placeholder="Enter password here">

<span class="help-block"><?php echo $password\_err; ?></span>

</div>

<div class="form-group <?php echo (!empty($confirm\_password\_err)) ? 'has-error' : ''; ?>">

<label>Confirm Password</label>

<input type="password" name="confirm\_password" class="form-control" value="<?php echo $confirm\_password; ?>" placeholder="Repeat password here">

<span class="help-block"><?php echo $confirm\_password\_err; ?></span>

</div>

<div class="form-group">

<br><button type="submit">Register</button>

</div>

</div>

</form>

</div>

</body>

</html>

**reset\_password.php**

<?php

$page\_title = 'Reset Password';

include ('./includes/header.php');

require\_once ('./config.php');

//Check if the user is logged in, if not then redirect to login page

if (!isset($\_SESSION["loggedin"]) || $\_SESSION["loggedin"] !== true) {

header("location: login.php");

exit;

}

// Define variables and initialize with empty values

$new\_password = $confirm\_password = "";

$new\_password\_err = $confirm\_password\_err = "";

//Processing form data when form is submitted

if ($\_SERVER["REQUEST\_METHOD"] == "POST") {

//Validate new password

if (empty(trim($\_POST["new\_password"]))) {

$new\_password\_err = "Please enter the new password.";

} elseif (strlen(trim($\_POST["new\_password"])) < 6) {

$new\_password\_err = "Password must have atleast 6 characters.";

} else {

$new\_password = trim($\_POST["new\_password"]);

}

//Validate confirm password

if (empty(trim($\_POST["confirm\_password"]))) {

$confirm\_password\_err = "Please confirm the password.";

} else {

$confirm\_password = trim($\_POST["confirm\_password"]);

if (empty($new\_password\_err) && ($new\_password != $confirm\_password)) {

$confirm\_password\_err = "Password did not match.";

}

}

//Check input errors before updating the database

if (empty($new\_password\_err) && empty($confirm\_password\_err)) {

//Prepare an update statement

$sql = "UPDATE entity\_user SET password = ? WHERE user\_id = ?";

if ($stmt = mysqli\_prepare($link, $sql)) {

//Bind variables to the prepared statement as parameters

mysqli\_stmt\_bind\_param($stmt, "si", $param\_password, $param\_id);

//Set parameters

$param\_password = password\_hash($new\_password, PASSWORD\_DEFAULT);

$param\_id = $\_SESSION["id"];

//Attempt to execute the prepared statement

if (mysqli\_stmt\_execute($stmt)) {

// Password updated successfully. Destroy the session, and redirect to login page

session\_destroy();

header("location: login.php");

exit();

} else {

echo "Oops! Something went wrong. Please try again later.";

}

}

//Close statement

mysqli\_stmt\_close($stmt);

}

//Close connection

mysqli\_close($link);

}

?>

<div id="accountForm">

<div class="container">

<h2>Reset Password</h2>

<hr>

<form action="<?php echo htmlspecialchars($\_SERVER["PHP\_SELF"]); ?>" method="post">

<div class="form-group <?php echo (!empty($new\_password\_err)) ? 'has-error' : ''; ?>">

<label>New Password</label>

<input type="password" name="new\_password" class="form-control" value="<?php echo $new\_password; ?>">

<span class="help-block"><?php echo $new\_password\_err; ?></span>

</div>

<div class="form-group <?php echo (!empty($confirm\_password\_err)) ? 'has-error' : ''; ?>">

<label>Confirm Password</label>

<input type="password" name="confirm\_password" class="form-control">

<span class="help-block"><?php echo $confirm\_password\_err; ?></span>

</div>

<div class="form-group">

<input type="submit" class="btn btn-primary" value="Submit">

<?php

if (isset($\_SESSION['admin']) && $\_SESSION['admin'] == true)

$string = "/Storefront/admin/admin.php";

else

$string = "/Storefront/account.php";

?>

<a class="btn btn-link" href="<?php echo $string ?>">Cancel</a>

</div>

</form>

</div>

</div>

</body>

</html>

**stylesheet.css**

body {

font-family: 'Roboto Slab', serif;

padding-bottom: 5%;

}

\* {

box-sizing: border-box;

}

#title {

margin: auto;

}

input[type=number] {

text-align: center;

}

input[type=text], input[type=password], input[type=box], textarea, select {

width: 100%;

padding: 15px;

margin: 5px 0 10px 0;

display: inline-block;

border: none;

background: #f1f1f1;

}

input[type=text]:focus, input[type=password]:focus, textarea:focus {

background-color: #ddd;

outline: none;

}

hr {

border: 1px solid #f1f1f1;

margin-bottom: 30px;

}

button:hover {

opacity: 1;

}

.container-fluid {

padding-left: 15%;

padding-right: 15%;

}

#error {

color: red;

border-style: solid;

display: none;

padding: 10px;

margin-bottom: 30px;

}

.settings {

padding-top: 10%;

padding-bottom: 5%;

}

.text-center {

margin-top: 5%;

padding-bottom: 1%;

}

table {

table-layout: fixed;

border-collapse: collapse;

width: 50%;

}

th, td {

text-align: center;

height: 50px;

}

tr:nth-child(even) {background-color: #F8F8F8;}

#accountForm {

position: relative;

margin: auto;

padding: 20px;

top: 0;

right: 0;

bottom: 50px;

left: 0;

max-width: 500px;

border-radius: 3px;

border: 1px solid #ccc;

}

#lblCartCount {

font-size: 12px;

background: #ff0000;

color: #fff;

padding: 0 5px;

vertical-align: top;

}

.center {

display: block;

margin-left: auto;

margin-right: auto;

}

table.tcenter {

margin-left: auto;

margin-right: auto;

}

div.form {

display: block;

text-align: center;

}

form {

display: inline-block;

margin-left: auto;

margin-right: auto;

text-align: left;

}

.page-header {

text-align: center;

}

.error {

color: red;

font-weight: bold;

}

ul.pagination {

display: table;

margin: 0 auto;

}

div.catalog {

position: absolute;

margin: auto;

}

.navbar-default {

background-color: white;

}

.panel-footer {

background-color: white;

}

.item {

color: black;

}

.product\_container {

padding: 15px;

max-width: 1200px;

display: flex;

margin: 0 auto;

}

.container {

padding: 15px;

max-width: 450px;

}

/\* Product pages \*/

.left-column {

width: 65%;

position: relative;

}

.right-column {

width: 35%;

margin-top: 60px;

}

.left-column img {

width: 100%;

position: absolute;

left: 0;

top: 0;

}

.product-description {

border-bottom: 1px solid #E1E8EE;

padding-bottom:20px;

margin-bottom: 20px;

}

.size-choose {

margin-bottom: 20px;

}

.size-choose button {

border: 2px solid #E1E8EE;

border-radius: 6px;

padding: 13px 20px;

font-size: 14px;

color: #5E6977;

background-color: #fff;

cursor: pointer;

transition: all .5s;

}

.size-choose button:hover, .size-choose button:active, .size-choose button:focus, button.active {

border: 2px solid #86939E;

outline: none;

}

.product-size {

border-bottom: 1px solid #E1E8EE;

margin-bottom: 20px;

margin-top: 20px;

}

.product-price {

display: flex;

align-items: center;

}

.product-price span {

font-size: 26px;

font-weight: 300;

color: #43474D;

margin-right: 20px;

}

.cart-btn {

display: inline-block;

background-color: #7DC855;

border-radius: 6px;

font-size: 16px;

color: #FFFFFF;

padding: 12px 30px;

transition: all .5s;

margin-top: 20px;

}

.cart-btn:hover {

background-color: #64af3d;

}

/\* End of product pages \*/

img {

width: auto;

height: auto;

max-width: 100%;

}

.col-centered {

float: none;

margin-right: auto;

margin-left: auto;

}

panel {

color: #FFFFFF;

}

.footer {

padding: 1%;

margin-top: 15%;

margin-left: 15%;

margin-right: 15%;

background-color: #f1f1f1;

text-align: center;

}

#error {

margin-top: 25px;

width: 250px;

text-align: center;

}

.badge {

position: absolute;

top: 5%;

}

.order {

border-style: solid;

border-width: thin;

max-width: 800px;

margin: 0 auto;

}

**view\_cart.php**

<?php

//This page displays the contents of the shopping cart and lets user update cart contents

$page\_title = 'Shopping Cart';

include ('includes/header.php');

require\_once "config.php";

echo '<div class="page-header"><h2><b>Cart</b></h2></div>';

//GET method - removing cart items

if (isset($\_GET['vid']) && is\_numeric($\_GET['vid'])) {

$vid = $\_GET['vid'];

unset($\_SESSION['cart'][$vid]); //Remove item

header("location: view\_cart.php");

}

//Check if the form has been submitted to update cart

if ($\_SERVER['REQUEST\_METHOD'] == 'POST') {

//Change any quantities:

foreach ($\_POST['qty'] as $k => $v) {

$varID = (int)$k;

$qty = (int)$v;

//Remove quantity

if ($qty == 0) {

unset ($\_SESSION['cart'][$varID]);

//Update quantity

} elseif ($qty > 0) {

$\_SESSION['cart'][$varID]['quantity'] = $qty;

}

}

}

//Display the cart

if (!empty($\_SESSION['cart'])) {

//Query product details

$q = "SELECT `entity\_product`.`image`, `entity\_product\_variant`.`variant\_id`, `entity\_product`.`product\_name`, `enum\_size`.`size`, `entity\_product`.`product\_price` FROM `storefront`.`xref\_product\_variant\_product` AS `xref\_product\_variant\_product`, `storefront`.`entity\_product` AS `entity\_product`, `storefront`.`entity\_product\_variant` AS `entity\_product\_variant`, `storefront`.`enum\_product\_type` AS `enum\_product\_type`, `storefront`.`enum\_size` AS `enum\_size` WHERE `xref\_product\_variant\_product`.`product\_id` = `entity\_product`.`product\_id` AND `xref\_product\_variant\_product`.`product\_variant\_id` = `entity\_product\_variant`.`variant\_id` AND `entity\_product`.`type` = `enum\_product\_type`.`id` AND `entity\_product\_variant`.`variant\_size` = `enum\_size`.`size\_id` AND `entity\_product\_variant`.`variant\_id` IN (";

foreach ($\_SESSION['cart'] as $varID => $value) {

$q .= $varID . ','; //Add each product in cart to query

}

$q = substr($q, 0, -1) . ')';

$r = mysqli\_query($link, $q);

// Create a form and a table:

echo '<form action="view\_cart.php" method="post">

<table border="0" class="tcenter">

<tr>

<td width="20%"><b>Image</b></td>

<td width="30%"><b>Product</b></td>

<td width="10%"><b>Size</b></td>

<td width="20%"><b>Price</b></td>

<td width="10%"><b>Quantity</b></td>

<td width="25%"><b>Total Price</b></td>

<td width="10%"></td>

</tr>';

//Print each item

$total = 0; //Total cost of order

while ($row = mysqli\_fetch\_array ($r, MYSQLI\_ASSOC)) {

//Calculate the total and sub-totals

$subtotal = $\_SESSION['cart'][$row['variant\_id']]['quantity'] \* $row['product\_price']; //Quantity \* Price

$total += $subtotal;

//Print the row

echo "<tr>

<td><img height='100px;' width='300px;' src='./img/{$row['image']}'</td>

<td>{$row['product\_name']}</td>

<td>{$row['size']}</td>

<td>\${$row['product\_price']}</td>

<td><input type='number' style='width:50px;' min='0' max='99' name='qty[{$row['variant\_id']}]' value='{$\_SESSION['cart'][$row['variant\_id']]['quantity']}'/></td>

<td>$" . number\_format ($subtotal, 2) . "</td>

<td><a href='view\_cart.php?vid=" . $row['variant\_id'] . "'>Remove</a></td>

</tr>\n";

}

mysqli\_close($link); //Close database connection

//Print total, close table and form

echo '<td colspan="7"><h4><b>Order Total: $' . number\_format ($total, 2) . '</b></h4></div></td>

</table>

<div class="text-center">

<input type="submit" name="submit" value="Update Cart" />

</form><br><br>

<a href="checkout.php" class="cart-btn">Checkout</a></p>

</div>';

$\_SESSION['order\_total'] = number\_format($total, 2);

} else { //Message if cart is empty

echo '<p class="text-center">Your cart is currently empty</p>';

}

?>

**view\_order.php**

<?php

$page\_title = 'Orders';

include ('./includes/header.php');

require ('./config.php');

echo '<div class="page-header"><h2><b>Order History</b></h2></div>';

//Check that user is logged in, redirect if not

if (!isset($\_SESSION["loggedin"]) && $\_SESSION["loggedin"] !== true) {

header("location: /Storefront/login.php");

exit;

}

$userID = $\_SESSION['id'];

//Get order count from user

$qOrder = "SELECT `entity\_order`.`order\_id`, `entity\_user`.`user\_id`, `entity\_order`.`created\_at` FROM `storefront`.`xref\_user\_order` AS `xref\_user\_order`, `storefront`.`entity\_user` AS `entity\_user`, `storefront`.`entity\_order` AS `entity\_order` WHERE `xref\_user\_order`.`user\_id` = `entity\_user`.`user\_id` AND `xref\_user\_order`.`order\_id` = `entity\_order`.`order\_id` AND `entity\_user`.`user\_id` = $userID ORDER BY `entity\_order`.`created\_at` DESC";

$rOrder = mysqli\_query($link, $qOrder);

$numOrder = mysqli\_num\_rows($rOrder);

if ($numOrder > 0) {

$orders = array();

while ($re = mysqli\_fetch\_array($rOrder, MYSQLI\_BOTH)) {

array\_push($orders, $re['order\_id']);

}

for ($i=0; $i<count($orders); $i++) {

$q = "SELECT `entity\_order`.`order\_id`, `entity\_user`.`user\_id`, `entity\_product`.`product\_name`, `enum\_size`.`size`, `entity\_order\_item`.`order\_item\_quantity`, `entity\_order\_item`.`order\_item\_price`, `entity\_order`.`created\_at`, `entity\_order`.`order\_total` FROM `storefront`.`entity\_product` AS `entity\_product`, `storefront`.`enum\_product\_type` AS `enum\_product\_type`, `storefront`.`entity\_product\_variant` AS `entity\_product\_variant`, `storefront`.`enum\_size` AS `enum\_size`, `storefront`.`xref\_order\_item\_product\_variant` AS `xref\_order\_item\_product\_variant`, `storefront`.`entity\_order\_item` AS `entity\_order\_item`, `storefront`.`xref\_order\_order\_item` AS `xref\_order\_order\_item`, `storefront`.`entity\_order` AS `entity\_order`, `storefront`.`xref\_product\_variant\_product` AS `xref\_product\_variant\_product`, `storefront`.`xref\_user\_order` AS `xref\_user\_order`, `storefront`.`entity\_user` AS `entity\_user` WHERE `entity\_product`.`type` = `enum\_product\_type`.`id` AND `entity\_product\_variant`.`variant\_size` = `enum\_size`.`size\_id` AND `xref\_order\_item\_product\_variant`.`order\_item\_id` = `entity\_order\_item`.`order\_item\_id` AND `xref\_order\_item\_product\_variant`.`product\_variant\_id` = `entity\_product\_variant`.`variant\_id` AND `xref\_order\_order\_item`.`order\_id` = `entity\_order`.`order\_id` AND `xref\_order\_order\_item`.`order\_item\_id` = `entity\_order\_item`.`order\_item\_id` AND `xref\_product\_variant\_product`.`product\_id` = `entity\_product`.`product\_id` AND `xref\_product\_variant\_product`.`product\_variant\_id` = `entity\_product\_variant`.`variant\_id` AND `xref\_user\_order`.`user\_id` = `entity\_user`.`user\_id` AND `xref\_user\_order`.`order\_id` = `entity\_order`.`order\_id` AND `entity\_order`.`order\_id` = $orders[$i] AND `entity\_user`.`user\_id` = $userID";

$r = mysqli\_query($link, $q);

mysqli\_data\_seek($r, 0);

$row = $r->fetch\_assoc();

echo '<div class="order">

<fieldset style="margin-top:5%;">

<div style="display:inline-block; margin-left:5%;">

<legend style="font-size: 1.2em";>

<p>Order Reference: #' . $row["order\_id"] . '</p>

<p style="vertical-align:middle;">Date Processed: ' . $row["created\_at"] . '</p>

<p style="vertical-align:middle;">Order Total: $' . $row['order\_total'] . '</p><br>

</legend>

<p>Order Details:</p>

</div>';

echo '<table class="tcenter" style="width:90%; margin-bottom:5%;">

<th>Product</th>

<th>Size</th>

<th>Quantity</th>

<th>Price per unit</th>

<th>Total Price</th>';

mysqli\_data\_seek($r ,0);

while ($re = mysqli\_fetch\_array($r, MYSQLI\_BOTH)) {

echo '<tr><td>' . $re['product\_name'] . '</td>

<td>' . $re['size'] . '</td>

<td>' . $re['order\_item\_quantity'] . '</td>

<td>' . $re['order\_item\_price'] . '</td>

<td>' . $re['order\_item\_quantity'] \* $re['order\_item\_price'] . '</td></tr>';

}

echo'</table></fieldset></div><br>';

}

} else {

echo '<p class="text-center">No order history</p>';

}

mysqli\_close($link);