**Assignment-7**

**Name: Aditya Taware**

**Div: TY-D**

**Roll no: 38**

**------------------------------------------------------------------------------------------------**

Title: Design and develop a responsive website for an online book store using PHP and MySQL having 1) Home Page 2) Login Page 3) Catalogue Page: 4) Registration Page: (database).

index.php:

<html>

<meta http-equiv="Content-Type"'.' content="text/html; charset=utf8"/>

<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">

<link rel="stylesheet" href="style.css">

<body>

<?php

session\_start();

    if(isset($\_POST['ac'])){

        $servername = "localhost";

        $username = "root";

        $password = "pratik@04";

        $conn = new mysqli($servername, $username, $password);

        if ($conn->connect\_error) {

            die("Connection failed: " . $conn->connect\_error);

        }

        $sql = "USE bookstore";

        $conn->query($sql);

        $sql = "SELECT \* FROM book WHERE BookID = '".$\_POST['ac']."'";

        $result = $conn->query($sql);

        while($row = $result->fetch\_assoc()){

            $bookID = $row['BookID'];

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

            $price = $row['Price'];

        }

        $sql = "INSERT INTO cart(BookID, Quantity, Price, TotalPrice) VALUES('".$bookID."', ".$quantity.", ".$price.", Price \* Quantity)";

        $conn->query($sql);

    }

    if(isset($\_POST['delc'])){

        $servername = "localhost";

        $username = "root";

        $password = "pratik@04";

        $conn = new mysqli($servername, $username, $password);

        if ($conn->connect\_error) {

            die("Connection failed: " . $conn->connect\_error);

        }

        $sql = "USE bookstore";

        $conn->query($sql);

        $sql = "DELETE FROM cart";

        $conn->query($sql);

    }

    $servername = "localhost";

    $username = "root";

    $password = "pratik@04";

    $conn = new mysqli($servername, $username, $password);

    if ($conn->connect\_error) {

        die("Connection failed: " . $conn->connect\_error);

    }

    $sql = "USE bookstore";

    $conn->query($sql);

    $sql = "SELECT \* FROM book";

    $result = $conn->query($sql);

?>

<?php

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

    echo '<header>';

    echo '<blockquote>';

    echo '<a href="index.php"><img src="image/logo.png"></a>';

    echo '<form class="hf" action="logout.php"><input class="hi" type="submit" name="submitButton" value="Logout"></form>';

    echo '<form class="hf" action="edituser.php"><input class="hi" type="submit" name="submitButton" value="Edit Profile"></form>';

    echo '</blockquote>';

    echo '</header>';

}

if(!isset($\_SESSION['id'])){

    echo '<header>';

    echo '<blockquote>';

    echo '<a href="index.php"><img src="image/logo.png"></a>';

    echo '<form class="hf" action="Register.php"><input class="hi" type="submit" name="submitButton" value="Register"></form>';

    echo '<form class="hf" action="login.php"><input class="hi" type="submit" name="submitButton" value="Login"></form>';

    echo '</blockquote>';

    echo '</header>';

}

echo '<blockquote>';

    echo "<table id='myTable' style='width:80%; float:left'>";

    echo "<tr>";

    while($row = $result->fetch\_assoc()) {

        echo "<td>";

        echo "<table>";

        echo '<tr><td>'.'<img src="'.$row["Image"].'"width="80%">'.'</td></tr><tr><td style="padding: 5px;">Title: '.$row["BookTitle"].'</td></tr><tr><td style="padding: 5px;">ISBN: '.$row["ISBN"].'</td></tr><tr><td style="padding: 5px;">Author: '.$row["Author"].'</td></tr><tr><td style="padding: 5px;">Type: '.$row["Type"].'</td></tr><tr><td style="padding: 5px;">RM'.$row["Price"].'</td></tr><tr><td style="padding: 5px;">

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

        Quantity: <input type="number" value="1" name="quantity" style="width: 20%"/><br>

        <input type="hidden" value="'.$row['BookID'].'" name="ac"/>

        <input class="button" type="submit" value="Add to Cart"/>

        </form></td></tr>';

        echo "</table>";

        echo "</td>";

    }

    echo "</tr>";

    echo "</table>";

    $sql = "SELECT book.BookTitle, book.Image, cart.Price, cart.Quantity, cart.TotalPrice FROM book,cart WHERE book.BookID = cart.BookID;";

    $result = $conn->query($sql);

    echo "<table style='width:20%; float:right;'>";

    echo "<th style='text-align:left;'><i class='fa fa-shopping-cart' style='font-size:24px'></i> Cart <form style='float:right;' action='' method='post'><input type='hidden' name='delc'/><input class='cbtn' type='submit' value='Empty Cart'></form></th>";

    $total = 0;

    while($row = $result->fetch\_assoc()){

        echo "<tr><td>";

        echo '<img src="'.$row["Image"].'"width="20%"><br>';

        echo $row['BookTitle']."<br>RM".$row['Price']."<br>";

        echo "Quantity: ".$row['Quantity']."<br>";

        echo "Total Price: RM".$row['TotalPrice']."</td></tr>";

        $total += $row['TotalPrice'];

    }

    echo "<tr><td style='text-align: right;background-color: #f2f2f2;''>";

    echo "Total: <b>RM".$total."</b><center><form action='checkout.php' method='post'><input class='button' type='submit' name='checkout' value='CHECKOUT'></form></center>";

    echo "</td></tr>";

    echo "</table>";

    echo '</blockquote>';

?>

</body>

</html>

html>

**connectDB.php :**

<?php

$pdo=new PDO('mysql:host=localhost;port=3306;dbname=bookstore','root', 'pratik@04');

?>

**register.php :**

<?php

session\_start();

$nameErr = $emailErr = $genderErr = $addressErr = $icErr = $contactErr = $usernameErr = $passwordErr = "";

$name = $email = $gender = $address = $ic = $contact = $uname = $upassword = "";

$cID;

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

    if (empty($\_POST["name"])) {

        $nameErr = "Please enter your name";

    }else{

        if (!preg\_match("/^[a-zA-Z ]\*$/", $name)){

            $nameErr = "Only letters and white space allowed";

            $name = "";

        }else{

            $name = $\_POST['name'];

            if (empty($\_POST["uname"])) {

                $usernameErr = "Please enter your Username";

                $uname = "";

            }else{

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

                if (empty($\_POST["upassword"])) {

                    $passwordErr = "Please enter your Password";

                    $upassword = "";

                }else{

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

                    if (empty($\_POST["ic"])){

                        $icErr = "Please enter your IC number";

                    }else{

                        if(!preg\_match("/^[0-9 -]\*$/", $ic)){

                            $icErr = "Please enter a valid IC number";

                            $ic = "";

                        }else{

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

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

                                $emailErr = "Please enter your email address";

                            }else{

                                if (filter\_var($email, FILTER\_VALIDATE\_EMAIL)){

                                    $emailErr = "Invalid email format";

                                    $email = "";

                                }else{

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

                                    if (empty($\_POST["contact"])){

                                        $contactErr = "Please enter your phone number";

                                    }else{

                                        if(!preg\_match("/^[0-9 -]\*$/", $contact)){

                                            $contactErr = "Please enter a valid phone number";

                                            $contact = "";

                                        }else{

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

                                            if (empty($\_POST["gender"])){

                                                $genderErr = "\* Gender is required!";

                                                $gender = "";

                                            }else{

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

                                                if (empty($\_POST["address"])){

                                                    $addressErr = "Please enter your address";

                                                    $address = "";

                                                }else{

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

                                                    $servername = "localhost";

                                                    $username = "root";

                                                    $password = "pratik@04";

                                                    $conn = new mysqli($servername, $username, $password);

                                                    if ($conn->connect\_error) {

                                                        die("Connection failed: " . $conn->connect\_error);

                                                    }

                                                    $sql = "USE bookstore";

                                                    $conn->query($sql);

                                                    $sql = "INSERT INTO users(UserName, Password) VALUES('".$uname."', '".$upassword."')";

                                                    $conn->query($sql);

                                                    $sql = "SELECT UserID FROM users WHERE UserName = '".$uname."'";

                                                    $result = $conn->query($sql);

                                                    while($row = $result->fetch\_assoc()){

                                                        $id = $row['UserID'];

                                                    }

                                                    $sql = "INSERT INTO customer(CustomerName, CustomerPhone, CustomerIC, CustomerEmail, CustomerAddress, CustomerGender, UserID)

                                                    VALUES('".$name."', '".$contact."', '".$ic."', '".$email."', '".$address."', '".$gender."', ".$id.")";

                                                    $conn->query($sql);

                                                    header("Location:index.php");

                                                }

                                            }

                                        }

                                    }

                                }

                            }

                        }

                    }

                }

            }

        }

    }

}

function test\_input($data){

    $data = trim($data);

    $data = stripcslashes($data);

    $data = htmlspecialchars($data);

    return $data;

}

?>

<html>

<link rel="stylesheet" href="style.css">

<body>

<header>

<blockquote>

    <a href="index.php"><img src="image/logo.png"></a>

</blockquote>

</header>

<blockquote>

<div class="container">

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

    <h1>Register:</h1>

    Full Name:<br><input type="text" name="name" placeholder="Full Name">

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $nameErr;?></span><br><br>

    User Name:<br><input type="text" name="uname" placeholder="User Name">

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $usernameErr;?></span><br><br>

    New Password:<br><input type="password" name="upassword" placeholder="Password">

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $passwordErr;?></span><br><br>

    IC Number:<br><input type="text" name="ic" placeholder="xxxxxx-xx-xxxx">

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $icErr;?></span><br><br>

    E-mail:<br><input type="text" name="email" placeholder="example@email.com">

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $emailErr;?></span><br><br>

    Mobile Number:<br><input type="text" name="contact" placeholder="012-3456789">

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $contactErr;?></span><br><br>

    <label>Gender:</label><br>

    <input type="radio" name="gender" <?php if (isset($gender) && $gender == "Male") echo "checked";?> value="Male">Male

    <input type="radio" name="gender" <?php if (isset($gender) && $gender == "Female") echo "checked";?> value="Female">Female

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $genderErr;?></span><br><br>

    <label>Address:</label><br>

    <textarea name="address" cols="50" rows="5" placeholder="Address"></textarea>

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $addressErr;?></span><br><br>

    <input class="button" type="submit" name="submitButton" value="Submit">

    <input class="button" type="button" name="cancel" value="Cancel" onClick="window.location='index.php';" />

</form>

</div>

</blockquote>

</center>

</body>

</html>

**login.php :**

<html>

<link rel="stylesheet" href="style.css">

<body>

<header>

<blockquote>

    <a href="index.php"><img src="image/logo.png"></a>

</blockquote>

</header>

<blockquote>

<div class="container">

<center><h1>Login</h1></center>

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

    Username:<br><input type="text" name="username"/>

    <br><br>

    Password:<br><input type="password" name="pwd" />

    <br><br>

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

    <input class="button" type="button" name="cancel" value="Cancel" onClick="window.location='index.php';" />

</form>

</div>

<blockquote>

<?php

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

    if($\_GET['errcode']==1){

        echo '<span style="color: red;">Invalid username or password.</span>';

    }elseif($\_GET['errcode']==2){

        echo '<span style="color: red;">Please login.</span>';

    }

}

?>

</body>

</html>

**logout.php :**

<?php

session\_start();

session\_destroy();

header("Location:index.php");

?>

**checklogin.php :**

<?php

session\_start();

if(isset($\_POST['username'])&&isset($\_POST['pwd'])){

    $username=$\_POST['username'];

    $pwd = $\_POST['pwd'];

    include "connectDB.php";

     $sql="SELECT \* FROM Users WHERE UserName=:username AND Password = :pwd;";

     $stmt = $pdo->prepare($sql);

    $stmt->execute(array(

        ':username' => $username,

        ':pwd' => $pwd

     ));

    if($stmt->rowCount()>0){

        while ( $row = $stmt->fetch(PDO::FETCH\_ASSOC) ) {

            $\_SESSION['id']=$row['UserID'];

             }

        header("Location:index.php");

    }else{

        echo '<span style="color: red;">Login Fail</span>';

        header("Location:login.php?errcode=1");

    }

}

?>

**checkout.php :**

<html>

<body style="font-family:Arial; margin: 0 auto; background-color: #f2f2f2;">

<header>

<blockquote>

    <img src="image/logo.png">

    <input class="hi" style="float: right; margin: 2%;" type="button" name="cancel" value="Home" onClick="window.location='index.php';" />

</blockquote>

</header>

<?php

session\_start();

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

    $servername = "localhost";

    $username = "root";

    $password = "pratik@04";

    $conn = new mysqli($servername, $username, $password);

    if ($conn->connect\_error) {

        die("Connection failed: " . $conn->connect\_error);

    }

    $sql = "USE bookstore";

    $conn->query($sql);

    $sql = "SELECT CustomerID from customer WHERE UserID = ".$\_SESSION['id']."";

    $result = $conn->query($sql);

    while($row = $result->fetch\_assoc()){

        $cID = $row['CustomerID'];

    }

    $sql = "UPDATE cart SET CustomerID = ".$cID." WHERE 1";

    $conn->query($sql);

    $sql = "SELECT \* FROM cart";

    $result = $conn->query($sql);

    while($row = $result->fetch\_assoc()){

        $sql = "INSERT INTO `order`(CustomerID, BookID, DatePurchase, Quantity, TotalPrice, Status)

        VALUES(".$row['CustomerID'].", '".$row['BookID']

        ."', CURRENT\_TIME, ".$row['Quantity'].", ".$row['TotalPrice'].", 'N')";

        $conn->query($sql);

    }

    $sql = "DELETE FROM cart";

    $conn->query($sql);

    $sql = "SELECT customer.CustomerName, customer.CustomerIC, customer.CustomerGender, customer.CustomerAddress, customer.CustomerEmail, customer.CustomerPhone, book.BookTitle, book.Price, book.Image, `order`.`DatePurchase`, `order`.`Quantity`, `order`.`TotalPrice`

        FROM customer, book, `order`

        WHERE `order`.`CustomerID` = customer.CustomerID AND `order`.`BookID` = book.BookID AND `order`.`Status` = 'N' AND `order`.`CustomerID` = ".$cID."";

    $result = $conn->query($sql);

    echo '<div class="container">';

    echo '<blockquote>';

?>

<input class="button" style="float: right;" type="button" name="cancel" value="Continue Shopping" onClick="window.location='index.php';" />

<?php

    echo '<h2 style="color: #000;">Order Successful</h2>';

    echo "<table style='width:100%'>";

    echo "<tr><th>Order Summary</th>";

    echo "<th></th></tr>";

    $row = $result->fetch\_assoc();

    echo "<tr><td>Name: </td><td>".$row['CustomerName']."</td></tr>";

    echo "<tr><td>No.Number: </td><td>".$row['CustomerIC']."</td></tr>";

    echo "<tr><td>E-mail: </td><td>".$row['CustomerEmail']."</td></tr>";

    echo "<tr><td>Mobile Number: </td><td>".$row['CustomerPhone']."</td></tr>";

    echo "<tr><td>Gender: </td><td>".$row['CustomerGender']."</td></tr>";

    echo "<tr><td>Address: </td><td>".$row['CustomerAddress']."</td></tr>";

    echo "<tr><td>Date: </td><td>".$row['DatePurchase']."</td></tr>";

    echo "</blockquote>";

    $sql = "SELECT customer.CustomerName, customer.CustomerIC, customer.CustomerGender, customer.CustomerAddress, customer.CustomerEmail, customer.CustomerPhone, book.BookTitle, book.Price, book.Image, `order`.`DatePurchase`, `order`.`Quantity`, `order`.`TotalPrice`

        FROM customer, book, `order`

        WHERE `order`.`CustomerID` = customer.CustomerID AND `order`.`BookID` = book.BookID AND `order`.`Status` = 'N' AND `order`.`CustomerID` = ".$cID."";

    $result = $conn->query($sql);

    $total = 0;

    while($row = $result->fetch\_assoc()){

        echo "<tr><td style='border-top: 2px solid #ccc;'>";

        echo '<img src="'.$row["Image"].'"width="20%"></td><td style="border-top: 2px solid #ccc;">';

        echo $row['BookTitle']."<br>RM".$row['Price']."<br>";

        echo "Quantity: ".$row['Quantity']."<br>";

        echo "</td></tr>";

        $total += $row['TotalPrice'];

    }

    echo "<tr><td style='background-color: #ccc;'></td><td style='text-align: right;background-color: #ccc;''>Total Price: <b>RM".$total."</b></td></tr>";

    echo "</table>";

    echo "</div>";

    $sql = "UPDATE `order` SET Status = 'y' WHERE CustomerID = ".$cID."";

    $conn->query($sql);

}

$nameErr = $emailErr = $genderErr = $addressErr = $icErr = $contactErr = "";

$name = $email = $gender = $address = $ic = $contact = "";

$cID;

if(isset($\_POST['submitButton'])){

    if (empty($\_POST["name"])) {

        $nameErr = "Please enter your name";

    }else{

        if (!preg\_match("/^[a-zA-Z ]\*$/", $name)){

            $nameErr = "Only letters and white space allowed";

            $name = "";

        }else{

            $name = $\_POST['name'];

            if (empty($\_POST["ic"])){

                $icErr = "Please enter your IC number";

            }else{

                if(!preg\_match("/^[0-9 -]\*$/", $ic)){

                    $icErr = "Please enter a valid IC number";

                    $ic = "";

                }else{

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

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

                        $emailErr = "Please enter your email address";

                    }else{

                        if (filter\_var($email, FILTER\_VALIDATE\_EMAIL)){

                            $emailErr = "Invalid email format";

                            $email = "";

                        }else{

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

                            if (empty($\_POST["contact"])){

                                $contactErr = "Please enter your phone number";

                            }else{

                                if(!preg\_match("/^[0-9 -]\*$/", $contact)){

                                    $contactErr = "Please enter a valid phone number";

                                    $contact = "";

                                }else{

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

                                    if (empty($\_POST["gender"])){

                                        $genderErr = "\* Gender is required!";

                                        $gender = "";

                                    }else{

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

                                        if (empty($\_POST["address"])){

                                            $addressErr = "Please enter your address";

                                            $address = "";

                                        }else{

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

                                            $servername = "localhost";

                                            $username = "root";

                                            $password = "";

                                            $conn = new mysqli($servername, $username, $password);

                                            if ($conn->connect\_error) {

                                                die("Connection failed: " . $conn->connect\_error);

                                            }

                                            $sql = "USE bookstore";

                                            $conn->query($sql);

                                            $sql = "INSERT INTO customer(CustomerName, CustomerPhone, CustomerIC, CustomerEmail, CustomerAddress, CustomerGender)

                                            VALUES('".$name."', '".$contact."', '".$ic."', '".$email."', '".$address."', '".$gender."')";

                                            $conn->query($sql);

                                            $sql = "SELECT CustomerID from customer WHERE CustomerName = '".$name."' AND CustomerIC = '".$ic."'";

                                            $result = $conn->query($sql);

                                            while($row = $result->fetch\_assoc()){

                                                $cID = $row['CustomerID'];

                                            }

                                            $sql = "UPDATE cart SET CustomerID = ".$cID." WHERE 1";

                                            $conn->query($sql);

                                            $sql = "SELECT \* FROM cart";

                                            $result = $conn->query($sql);

                                            while($row = $result->fetch\_assoc()){

                                                $sql = "INSERT INTO `order`(CustomerID, BookID, DatePurchase, Quantity, TotalPrice, Status)

                                                VALUES(".$row['CustomerID'].", '".$row['BookID']

                                                ."', CURRENT\_TIME, ".$row['Quantity'].", ".$row['TotalPrice'].", 'N')";

                                                $conn->query($sql);

                                            }

                                            $sql = "DELETE FROM cart";

                                            $conn->query($sql);

                                        }

                                    }

                                }

                            }

                        }

                    }

                }

            }

        }

    }

}

function test\_input($data){

    $data = trim($data);

    $data = stripcslashes($data);

    $data = htmlspecialchars($data);

    return $data;

}

?>

<style>

header {

    background-color: rgb(0,51,102);

    width: 100%;

}

header img {

    margin: 1%;

}

header .hi{

    background-color: #fff;

    border: none;

    border-radius: 20px;

    text-align: center;

    transition-duration: 0.5s;

    padding: 8px 30px;

    cursor: pointer;

    color: #000;

    margin-top: 15%;

}

header .hi:hover{

    background-color: #ccc;

}

form{

    margin-top: 1%;

    float: left;

    width: 40%;

    color: #000;

}

input[type=text] {

    padding: 5px;

    border-radius: 3px;

    box-sizing: border-box;

    border: 2px solid #ccc;

    transition: 0.5s;

    outline: none;

}

input[type=text]:focus {

    border: 2px solid rgb(0,51,102);

}

textarea {

    outline: none;

    border: 2px solid #ccc;

}

textarea:focus {

    border: 2px solid rgb(0,51,102);

}

.button{

    background-color: rgb(0,51,102);

    border: none;

    border-radius: 20px;

    text-align: center;

    transition-duration: 0.5s;

    padding: 8px 30px;

    cursor: pointer;

    color: #fff;

}

.button:hover {

    background-color: rgb(102,255,255);

    color: #000;

}

table {

    border-collapse: collapse;

    width: 60%;

    float: right;

}

th, td {

    text-align: left;

    padding: 8px;

}

tr{background-color: #fff;}

th {

    background-color: rgb(0,51,102);

    color: white;

}

.container {

    width: 50%;

    border-radius: 5px;

    background-color: #f2f2f2;

    padding: 20px;

    margin: 0 auto;

}

</style>

<blockquote>

<?php

if(!isset($\_SESSION['id'])){

    echo "<form method='post'  action=''>";

    echo 'Name:<br><input type="text" name="name" placeholder="Full Name">';

    echo '<span class="error" style="color: red; font-size: 0.8em;"><?php echo $nameErr;?></span><br><br>';

    echo 'IC Number:<br><input type="text" name="ic" placeholder="xxxxxx-xx-xxxx">';

    echo '<span class="error" style="color: red; font-size: 0.8em;"><?php echo $icErr;?></span><br><br>';

    echo 'E-mail:<br><input type="text" name="email" placeholder="example@email.com">';

    echo '<span class="error" style="color: red; font-size: 0.8em;"><?php echo $emailErr;?></span><br><br>';

    echo 'Mobile Number:<br><input type="text" name="contact" placeholder="012-3456789">';

    echo '<span class="error" style="color: red; font-size: 0.8em;"><?php echo $contactErr;?></span><br><br>';

    echo '<label>Gender:</label><br>';

    echo '<input type="radio" name="gender" if (isset($gender) && $gender == "Male") echo "checked"; value="Male">Male';

    echo '<input type="radio" name="gender" if (isset($gender) && $gender == "Female") echo "checked"; value="Female">Female';

    echo '<span class="error" style="color: red; font-size: 0.8em;"><?php echo $genderErr;?></span><br><br>';

    echo '<label>Address:</label><br>';

       echo '<textarea name="address" cols="30" rows="5" placeholder="Address"></textarea>';

       echo '<span class="error" style="color: red; font-size: 0.8em;"><?php echo $addressErr;?></span><br><br>';

?>

<input class="button" type="button" name="cancel" value="Cancel" onClick="window.location='index.php';" />

<?php

    echo '<input class="button" type="submit" name="submitButton" value="CHECKOUT">';

    echo '</form><br><br>';

}

if(isset($\_POST['submitButton'])){

    $servername = "localhost";

    $username = "root";

    $password = "";

    $conn = new mysqli($servername, $username, $password);

    if ($conn->connect\_error) {

        die("Connection failed: " . $conn->connect\_error);

    }

    $sql = "USE bookstore";

    $conn->query($sql);

    $sql = "SELECT customer.CustomerName, customer.CustomerIC, customer.CustomerGender, customer.CustomerAddress, customer.CustomerEmail, customer.CustomerPhone, book.BookTitle, book.Price, book.Image, `order`.`DatePurchase`, `order`.`Quantity`, `order`.`TotalPrice`

        FROM customer, book, `order`

        WHERE `order`.`CustomerID` = customer.CustomerID AND `order`.`BookID` = book.BookID AND `order`.`Status` = 'N' AND `order`.`CustomerID` = ".$cID."";

    $result = $conn->query($sql);

    echo '<table style="width: 40%">';

    echo "<tr><th>Order Summary</th>";

    echo "<th></th></tr>";

    $row = $result->fetch\_assoc();

    echo "<tr><td>Name: </td><td>".$row['CustomerName']."</td></tr>";

    echo "<tr><td>No.Number: </td><td>".$row['CustomerIC']."</td></tr>";

    echo "<tr><td>E-mail: </td><td>".$row['CustomerEmail']."</td></tr>";

    echo "<tr><td>Mobile Number: </td><td>".$row['CustomerPhone']."</td></tr>";

    echo "<tr><td>Gender: </td><td>".$row['CustomerGender']."</td></tr>";

    echo "<tr><td>Address: </td><td>".$row['CustomerAddress']."</td></tr>";

    echo "<tr><td>Date: </td><td>".$row['DatePurchase']."</td></tr>";

    $sql = "SELECT customer.CustomerName, customer.CustomerIC, customer.CustomerGender, customer.CustomerAddress, customer.CustomerEmail, customer.CustomerPhone, book.BookTitle, book.Price, book.Image, `order`.`DatePurchase`, `order`.`Quantity`, `order`.`TotalPrice`

        FROM customer, book, `order`

        WHERE `order`.`CustomerID` = customer.CustomerID AND `order`.`BookID` = book.BookID AND `order`.`Status` = 'N' AND `order`.`CustomerID` = ".$cID."";

    $result = $conn->query($sql);

    $total = 0;

    while($row = $result->fetch\_assoc()){

        echo "<tr><td style='border-top: 2px solid #ccc;'>";

        echo '<img src="'.$row["Image"].'"width="20%"></td><td style="border-top: 2px solid #ccc;">';

        echo $row['BookTitle']."<br>RM".$row['Price']."<br>";

        echo "Quantity: ".$row['Quantity']."<br>";

        echo "</td></tr>";

        $total += $row['TotalPrice'];

    }

    echo "<tr><td style='background-color: #ccc;'></td><td style='text-align: right;background-color: #ccc;'>Total Price: <b>RM".$total."</b></td></tr>";

    echo "</table>";

    $sql = "UPDATE `order` SET Status = 'y' WHERE CustomerID = ".$cID."";

    $conn->query($sql);

}

?>

</blockquote>

</body>

</html>

**edituser.php :**

<?php

session\_start();

$nameErr = $emailErr = $genderErr = $addressErr = $icErr = $contactErr = $usernameErr = $passwordErr = "";

$name = $email = $gender = $address = $ic = $contact = $uname = $upassword = "";

$cID;

$oUserName;

$oPassword;

$oName;

$oIC;

$oEmail;

$oPhone;

$oAddress;

$servername = "localhost";

$username = "root";

$password = "pratik@04";

$conn = new mysqli($servername, $username, $password);

if ($conn->connect\_error) {

    die("Connection failed: " . $conn->connect\_error);

}

$sql = "USE bookstore";

$conn->query($sql);

$sql = "SELECT users.UserName, users.Password, customer.CustomerName, customer.CustomerIC, customer.CustomerEmail, customer.CustomerPhone, customer.CustomerGender, customer.CustomerAddress

    FROM users, customer

    WHERE users.UserID = customer.UserID AND users.UserID = ".$\_SESSION['id']."";

$result = $conn->query($sql);

while($row = $result->fetch\_assoc()){

    $oUserName = $row['UserName'];

    $oPassword = $row['Password'];

    $oName = $row['CustomerName'];

    $oIC = $row['CustomerIC'];

    $oEmail = $row['CustomerEmail'];

    $oPhone = $row['CustomerPhone'];

    $oAddress = $row['CustomerAddress'];

}

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

    if (empty($\_POST["name"])) {

        $nameErr = "Please enter your name";

    }else{

        if (!preg\_match("/^[a-zA-Z ]\*$/", $name)){

            $nameErr = "Only letters and white space allowed";

            $name = "";

        }else{

            $name = $\_POST['name'];

            if (empty($\_POST["uname"])) {

                $usernameErr = "Please enter your Username";

                $uname = "";

            }else{

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

                if (empty($\_POST["upassword"])) {

                    $passwordErr = "Please enter your Password";

                    $upassword = "";

                }else{

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

                    if (empty($\_POST["ic"])){

                        $icErr = "Please enter your IC number";

                    }else{

                        if(!preg\_match("/^[0-9 -]\*$/", $ic)){

                            $icErr = "Please enter a valid IC number";

                            $ic = "";

                        }else{

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

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

                                $emailErr = "Please enter your email address";

                            }else{

                                if (filter\_var($email, FILTER\_VALIDATE\_EMAIL)){

                                    $emailErr = "Invalid email format";

                                    $email = "";

                                }else{

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

                                    if (empty($\_POST["contact"])){

                                        $contactErr = "Please enter your phone number";

                                    }else{

                                        if(!preg\_match("/^[0-9 -]\*$/", $contact)){

                                            $contactErr = "Please enter a valid phone number";

                                            $contact = "";

                                        }else{

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

                                            if (empty($\_POST["gender"])){

                                                $genderErr = "\* Gender is required!";

                                                $gender = "";

                                            }else{

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

                                                if (empty($\_POST["address"])){

                                                    $addressErr = "Please enter your address";

                                                    $address = "";

                                                }else{

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

                                                    $servername = "localhost";

                                                    $username = "root";

                                                    $password = "";

                                                    $conn = new mysqli($servername, $username, $password);

                                                    if ($conn->connect\_error) {

                                                        die("Connection failed: " . $conn->connect\_error);

                                                    }

                                                    $sql = "USE bookstore";

                                                    $conn->query($sql);

                                                    $sql = "UPDATE users SET UserName = '".$uname."', Password = '".$upassword."' WHERE UserID = "

                                                    .$\_SESSION['id']."";

                                                    $conn->query($sql);

                                                    $sql = "UPDATE customer SET CustomerName = '".$name."', CustomerPhone = '".$contact."',

                                                    CustomerIC = '".$ic."', CustomerEmail = '".$email."', CustomerAddress = '".$address."',

                                                    CustomerGender = '".$gender."'";

                                                    $conn->query($sql);

                                                    header("Location:index.php");

                                                }

                                            }

                                        }

                                    }

                                }

                            }

                        }

                    }

                }

            }

        }

    }

}

function test\_input($data){

    $data = trim($data);

    $data = stripcslashes($data);

    $data = htmlspecialchars($data);

    return $data;

}

?>

<html>

<link rel="stylesheet" href="style.css">

<body>

<header>

<blockquote>

    <a href="index.php"><img src="image/logo.png"></a>

</blockquote>

</header>

<blockquote>

<div class="container">

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

    <h1>Edit Profile:</h1>

    Full Name:<br><input type="text" name="name" placeholder="<?php echo $oName; ?>">

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $nameErr;?></span><br><br>

    User Name:<br><input type="text" name="uname" placeholder="<?php echo $oUserName; ?>">

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $usernameErr;?></span><br><br>

    New Password:<br><input type="password" name="upassword" placeholder="<?php echo $oPassword; ?>">

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $passwordErr;?></span><br><br>

    IC Number:<br><input type="text" name="ic" placeholder="<?php echo $oIC; ?>">

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $icErr;?></span><br><br>

    E-mail:<br><input type="text" name="email" placeholder="<?php echo $oEmail; ?>">

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $emailErr;?></span><br><br>

    Mobile Number:<br><input type="text" name="contact" placeholder="<?php echo $oPhone; ?>">

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $contactErr;?></span><br><br>

    <label>Gender:</label><br>

    <input type="radio" name="gender" <?php if (isset($gender) && $gender == "Male") echo "checked";?> value="Male">Male

    <input type="radio" name="gender" <?php if (isset($gender) && $gender == "Female") echo "checked";?> value="Female">Female

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $genderErr;?></span><br><br>

    <label>Address:</label><br>

    <textarea name="address" cols="50" rows="5" placeholder="<?php echo $oAddress; ?>"></textarea>

    <span class="error" style="color: red; font-size: 0.8em;"><?php echo $addressErr;?></span><br><br>

    <input class="button" type="submit" name="submitButton" value="Edit">

    <input class="button" type="button" name="cancel" value="Cancel" onClick="window.location='index.php';" />

</form>

</div>

</blockquote>

</center>

</body>

</html>

**style.css :**

body{

    font-family: Arial;

    margin: 0 auto;

}

header {

    background-color: rgb(0,51,102);

    width: 100%;

}

header img {

    margin: 1%;

}

header .hf{

    float: right;

    margin: 1.5%;

}

header .hi{

    background-color: #fff;

    border: none;

    border-radius: 20px;

    text-align: center;

    transition-duration: 0.5s;

    padding: 8px 30px;

    cursor: pointer;

    color: #000;

    font-weight: bold;

    margin-top: 15%;

}

header .hi:hover{

    background-color: #ccc;

}

table {

    border-collapse: collapse;

}

tr{background-color: #fff;}

th {

    padding-top: 12px;

    padding-bottom: 12px;

    text-align: left;

    background-color: rgb(0,51,102);

    color: white;

}

table .btn{

    background-color: #ec7115;

    border: none;

    text-align: center;

    transition-duration: 0.5s;

    padding: 8px 30px;

    cursor: pointer;

    color: #fff;

    margin-top: 5%;

}

table .btn:hover{

    background-color: #e3e3e3;

    color: #ec7115;

}

.button{

    background-color: rgb(0,51,102);

    border: none;

    border-radius: 20px;

    text-align: center;

    transition-duration: 0.5s;

    padding: 8px 30px;

    cursor: pointer;

    color: #fff;

    margin-top: 5%;

    font-weight: bold;

}

.button:hover {

    background-color: rgb(102,255,255);

    color: #000;

}

.cbtn{

    background-color: #fff;

    border: none;

    border-radius: 20px;

    text-align: center;

    transition-duration: 0.5s;

    padding: 8px 30px;

    cursor: pointer;

    color: #000;

    font-weight: bold;

}

.cbtn:hover{

    background-color: #ccc;

}

form{

    margin-top: 2%;

}

input[type=text], input[type=password]{

    width: 100%;

    padding: 12px;

    border-radius: 3px;

    box-sizing: border-box;

    border: 2px solid #ccc;

    transition: 0.5s;

    outline: none;

}

input[type=text]:focus, input[type=password]:focus {

    border: 2px solid rgb(0,51,102);

}

textarea {

    outline: none;

    border: 2px solid #ccc;

}

textarea:focus {

    border: 2px solid rgb(0,51,102);

}

.container {

    width: 55%;

    border-radius: 5px;

    background-color: #f2f2f2;

    padding: 20px;

    margin: 0 auto;

}

**database.sql :**

CREATE DATABASE BookStore;

USE BookStore;

CREATE TABLE Book(

    BookID varchar(50),

    BookTitle varchar(200),

    ISBN varchar(20),

    Price double(12,2),

    Author varchar(128),

    Type varchar(128),

    Image varchar(128),

    PRIMARY KEY (BookID)

);

CREATE TABLE Users(

    UserID int not null AUTO\_INCREMENT,

    UserName varchar(128),

    Password varchar(16),

    PRIMARY KEY (UserID)

);

CREATE TABLE Customer (

    CustomerID int not null AUTO\_INCREMENT,

    CustomerName varchar(128),

    CustomerPhone varchar(12),

    CustomerIC varchar(14),

    CustomerEmail varchar(200),

    CustomerAddress varchar(200),

    CustomerGender varchar(10),

    UserID int,

    PRIMARY KEY (CustomerID),

    CONSTRAINT FOREIGN KEY (UserID) REFERENCES Users(UserID) ON DELETE SET NULL ON UPDATE CASCADE

);

CREATE TABLE `Order`(

    OrderID int not null AUTO\_INCREMENT,

    CustomerID int,

    BookID varchar(50),

    DatePurchase datetime,

    Quantity int,

    TotalPrice double(12,2),

    Status varchar(1),

    PRIMARY KEY (OrderID),

    CONSTRAINT FOREIGN KEY (BookID) REFERENCES Book(BookID) ON DELETE SET NULL ON UPDATE CASCADE,

    CONSTRAINT FOREIGN KEY (CustomerID) REFERENCES Customer(CustomerID) ON DELETE SET NULL ON UPDATE CASCADE

);

CREATE TABLE Cart(

    CartID int not null AUTO\_INCREMENT,

    CustomerID int,

    BookID varchar(50),

    Price double(12,2),

    Quantity int,

    TotalPrice double(12,2),

    PRIMARY KEY (CartID),

    CONSTRAINT FOREIGN KEY (BookID) REFERENCES Book(BookID) ON DELETE SET NULL ON UPDATE CASCADE,

    CONSTRAINT FOREIGN KEY (CustomerID) REFERENCES Customer(CustomerID) ON DELETE SET NULL ON UPDATE CASCADE

);

INSERT INTO `book`(`BookID`, `BookTitle`, `ISBN`, `Price`, `Author`, `Type`, `Image`) VALUES ('B-001','Lonely Planet Australia (Travel Guide)','123-456-789-1',136,'Lonely Planet','Travel','image/travel.jpg');

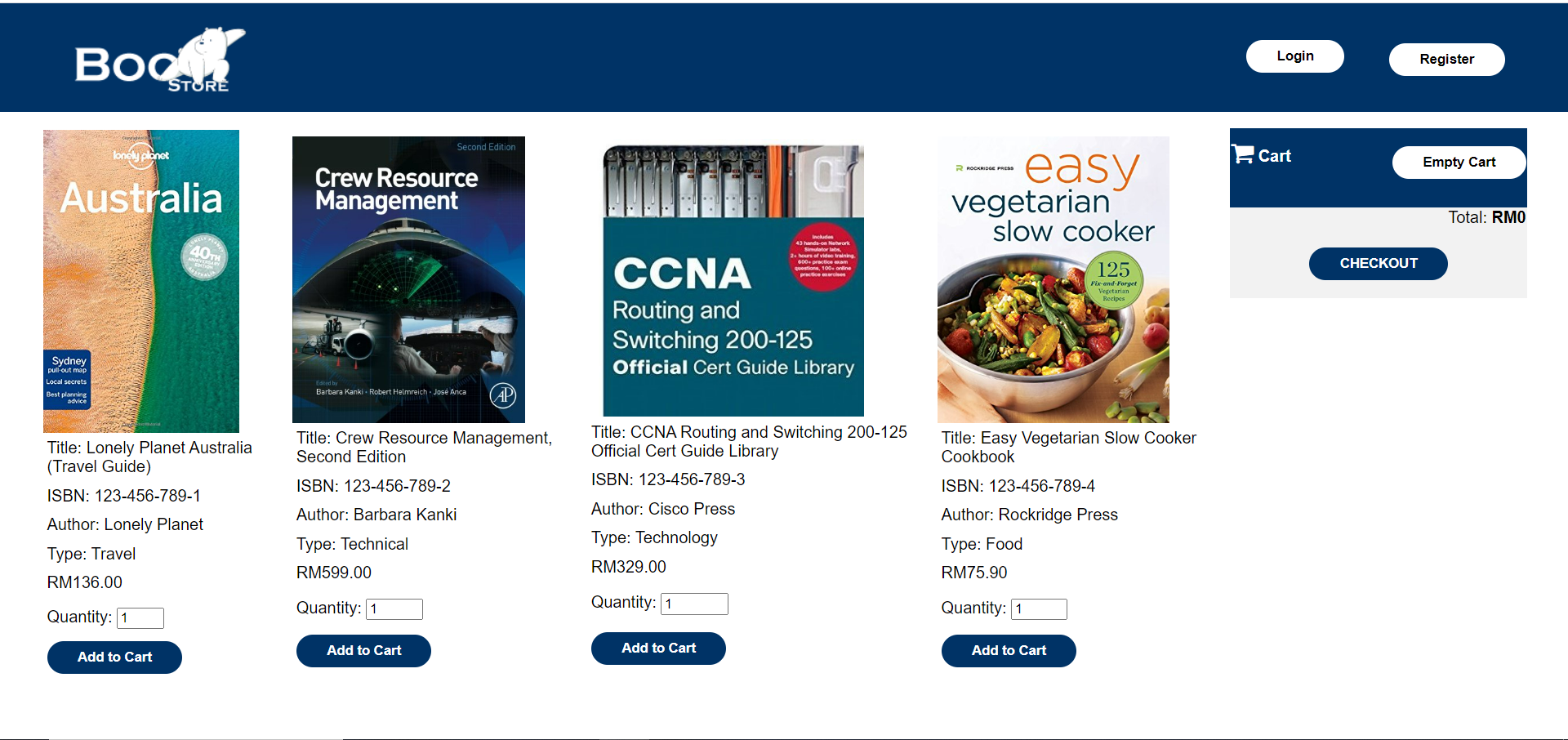
INSERT INTO `book`(`BookID`, `BookTitle`, `ISBN`, `Price`, `Author`, `Type`, `Image`) VALUES ('B-002','Crew Resource Management, Second Edition','123-456-789-2',599,'Barbara Kanki','Technical','image/technical.jpg');

INSERT INTO `book`(`BookID`, `BookTitle`, `ISBN`, `Price`, `Author`, `Type`, `Image`) VALUES ('B-003','CCNA Routing and Switching 200-125 Official Cert Guide Library','123-456-789-3',329,'Cisco Press ','Technology','image/technology.jpg');

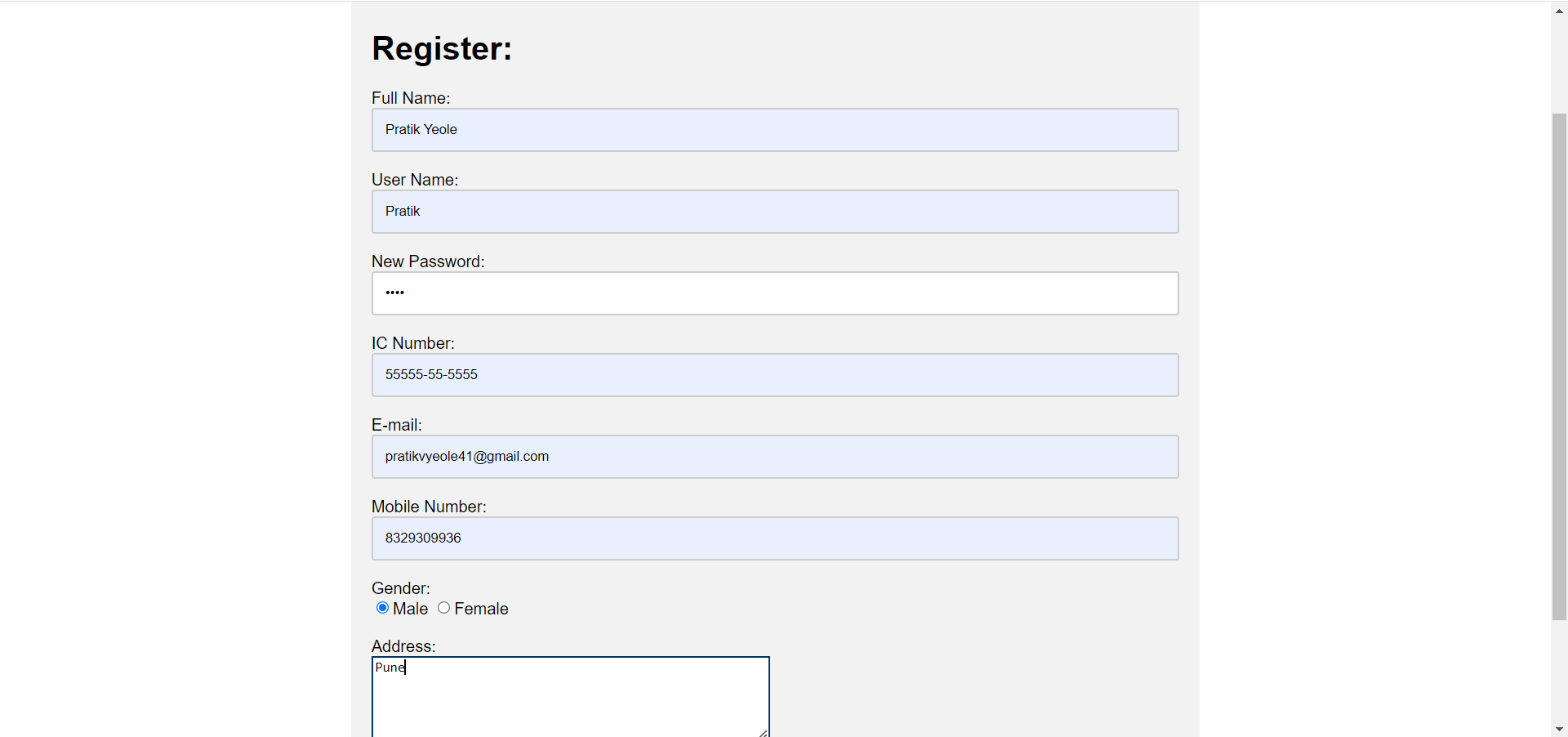
INSERT INTO `book`(`BookID`, `BookTitle`, `ISBN`, `Price`, `Author`, `Type`, `Image`) VALUES ('B-004','Easy Vegetarian Slow Cooker Cookbook','123-456-789-4',75.9,'Rockridge Press','Food','image/food.jpg');

**Output:**

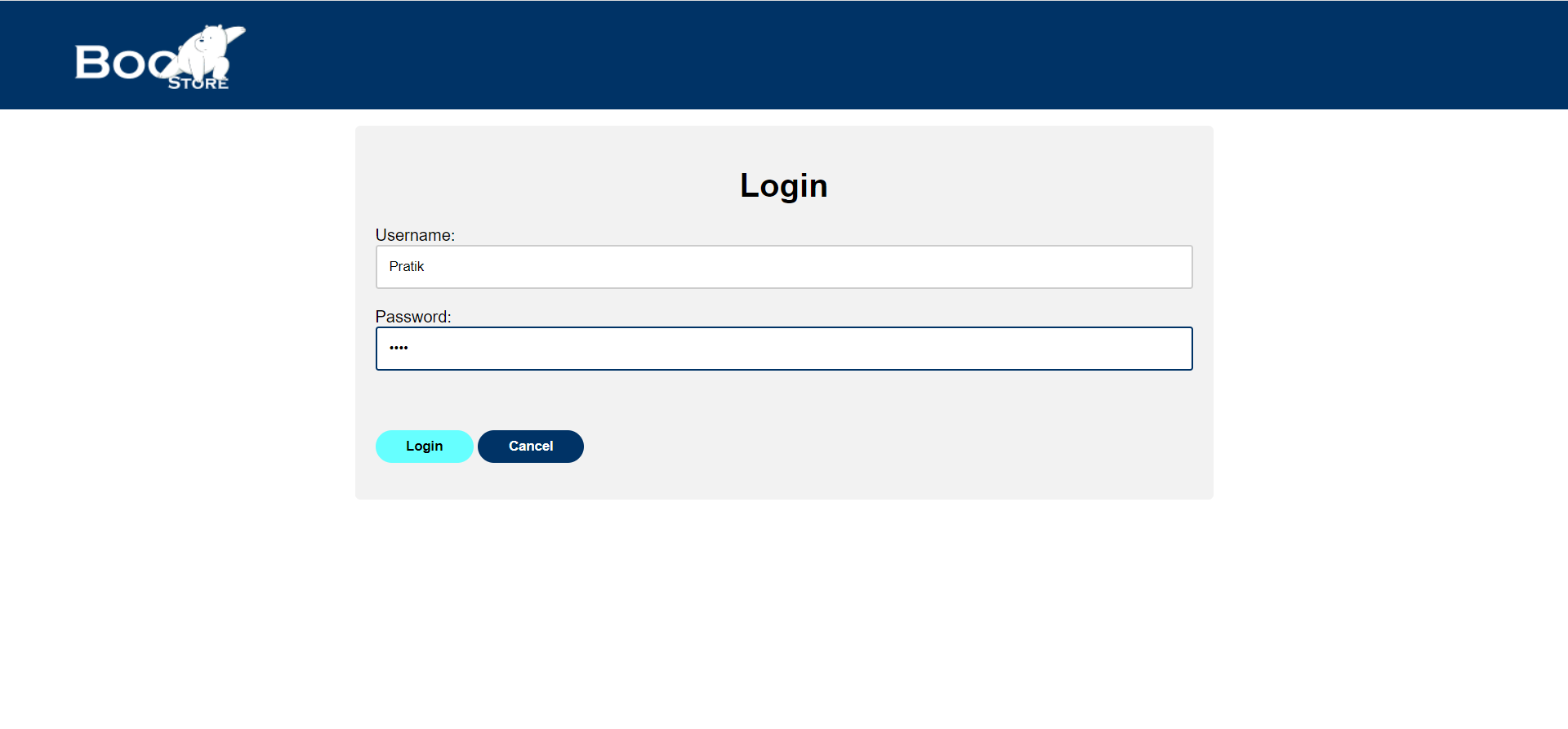
**Home Page:**



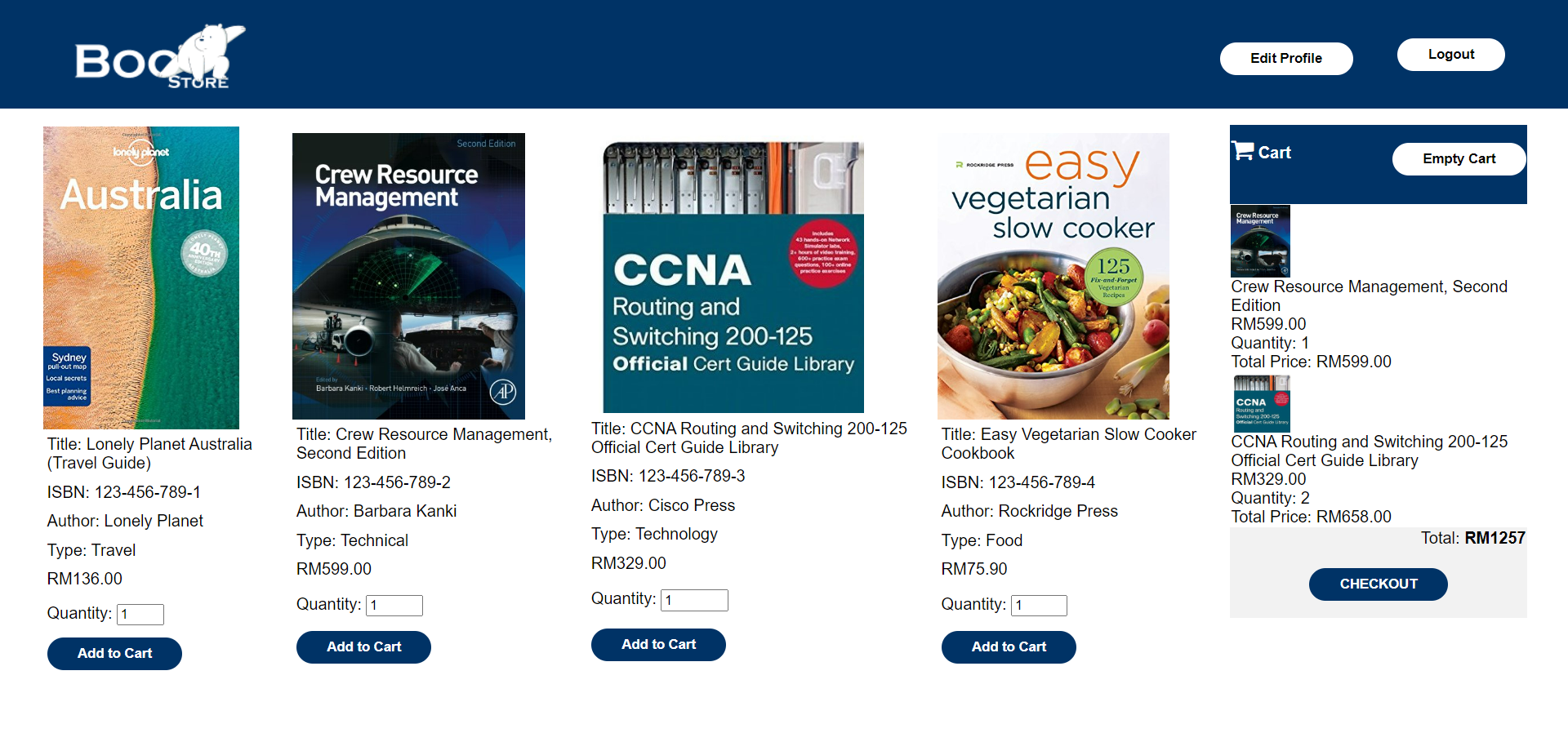
**Register Page:**



**Login Page:**



**After Login Home Page:**



**Checkout Page:**

