**Module 1: User Registration**

|  |
| --- |
| <?php  // Connect to DB  $conn = new mysqli('localhost', 'root', '', 'bookstore');  // Register User  if (isset($\_POST['register'])) {  $username = $\_POST['username'];  $password = $\_POST['password'];  $sql = "INSERT INTO users (username, password) VALUES ('$username', '$password')";  $conn->query($sql);  echo "User registered!";  }  // Login User  if (isset($\_POST['login'])) {  $username = $\_POST['username'];  $password = $\_POST['password'];  $sql = "SELECT \* FROM users WHERE username='$username' AND password='$password'";  $result = $conn->query($sql);  if ($result->num\_rows > 0) {  // No session management  echo "Login successful! Welcome, $username";  } else {  echo "Invalid credentials";  }  }  ?>  <form method="POST">  <h2>Register</h2>  Username: <input name="username"><br>  Password: <input name="password" type="password"><br>  <button name="register">Register</button>  </form>  <form method="POST">  <h2>Login</h2>  Username: <input name="username"><br>  Password: <input name="password" type="password"><br>  <button name="login">Login</button>  </form> |

**Module 2: Shopping Cart Management**

|  |
| --- |
| <?php  // Add to Cart  if (isset($\_GET['add'])) {  $book\_id = $\_GET['add'];  // Directly using book\_id without validation  echo "<p>Added book ID $book\_id to cart <p>";  }  // Remove from Cart  if (isset($\_GET['remove'])) {  $book\_id = $\_GET['remove'];  echo "<p>Removed book ID $book\_id from cart </p>";  }  ?>  <a href="?add=1">Add Book 1 to Cart</a> | <a href="?remove=1">Remove Book 1 from Cart</a> |

**Module 3: Checkout and Order Placement**

|  |
| --- |
| <?php  // Place order  if (isset($\_POST['checkout'])) {  $name = $\_POST['name'];  $address = $\_POST['address'];  $credit\_card = $\_POST['credit\_card'];  $sql = "INSERT INTO orders (name, address, credit\_card) VALUES ('$name', '$address', '$credit\_card')";  $conn->query($sql);  echo "Order placed successfully!";  }  ?>  <form method="POST">  Name: <input name="name"><br>  Address: <input name="address"><br>  Credit Card: <input name="credit\_card"><br>  <button name="checkout">Place Order</button>  </form> |

**Module 4: Order History and Tracking**

|  |
| --- |
| <?php  // View order by user\_id  if (isset($\_GET['user\_id'])) {  $user\_id = $\_GET['user\_id'];  $sql = "SELECT \* FROM orders WHERE user\_id = $user\_id";  $result = $conn->query($sql);  echo "<h2>Order History for User ID: $user\_id</h2><ul>";  while ($row = $result->fetch\_assoc()) {  echo "<li>Order ID: " . $row['id'] . " - Status: " . $row['status'] . "</li>";  }  echo "</ul>";  } else {  echo "No user\_id specified.";  }  ?> |

**Module 5: Admin Panel**

|  |
| --- |
| <?php  // List all books (no output encoding)  $sql = "SELECT \* FROM books";  $result = $conn->query($sql);  echo "<h2>Admin - Manage Books</h2><ul>";  while ($row = $result->fetch\_assoc()) {  echo "<li>ID: " . $row['id'] . " Title: " . $row['title'] . " - <a href='?delete=" . $row['id'] . "'>Delete</a></li>";  }  // Delete book  if (isset($\_GET['delete'])) {  $id = $\_GET['delete'];  $sql = "DELETE FROM books WHERE id = $id";  $conn->query($sql);  echo "Deleted book ID $id";  }  echo "</ul>";  ?> |