广东省第四届“强网杯”网络安全大赛（“泄露的秘密WP”）

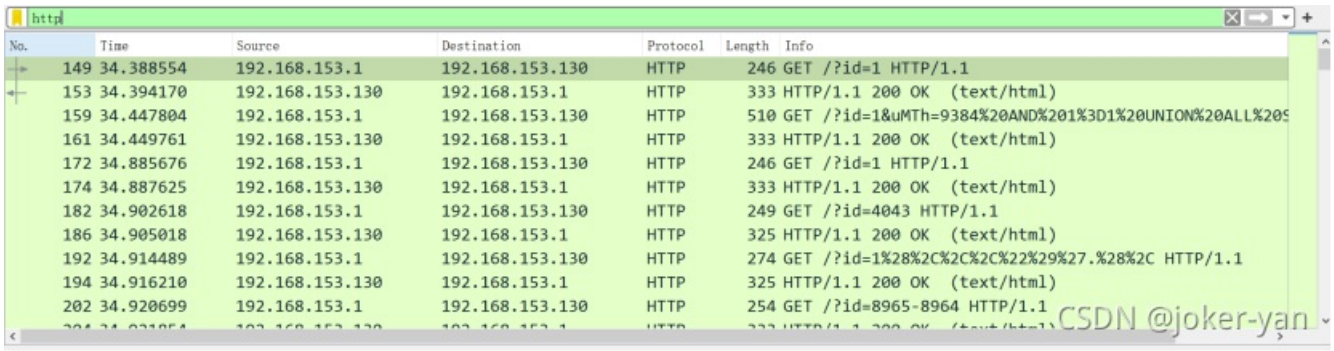
原创

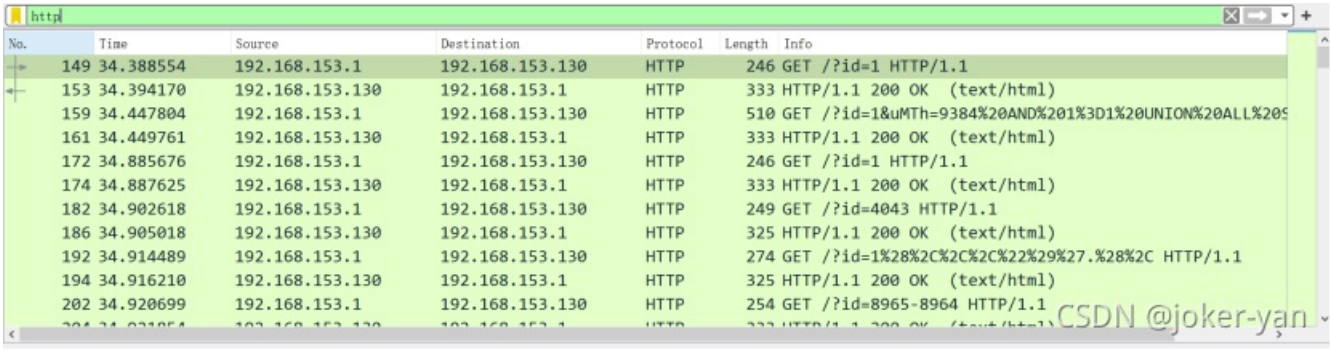
joker-yan 于 2021-10-14 15:11:28 发布 4268 收藏 1
分类专栏： CTF 强网杯 文章标签： 网络安全 python sql

感觉应该就算交了WP也进不了决赛~~

我直接把WP放这里

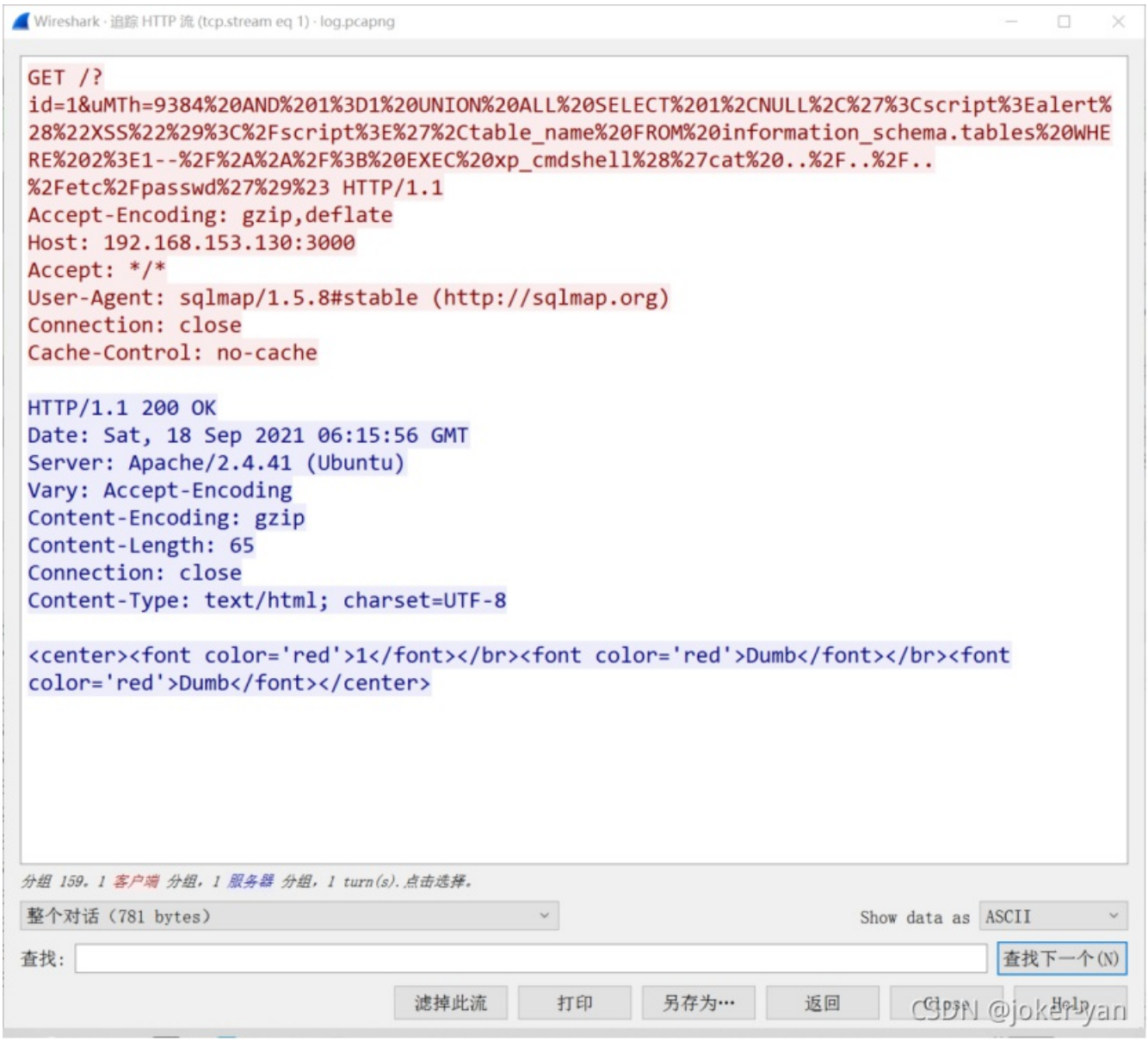
“泄露的秘密”:





发现存在大量“HTTP”包。

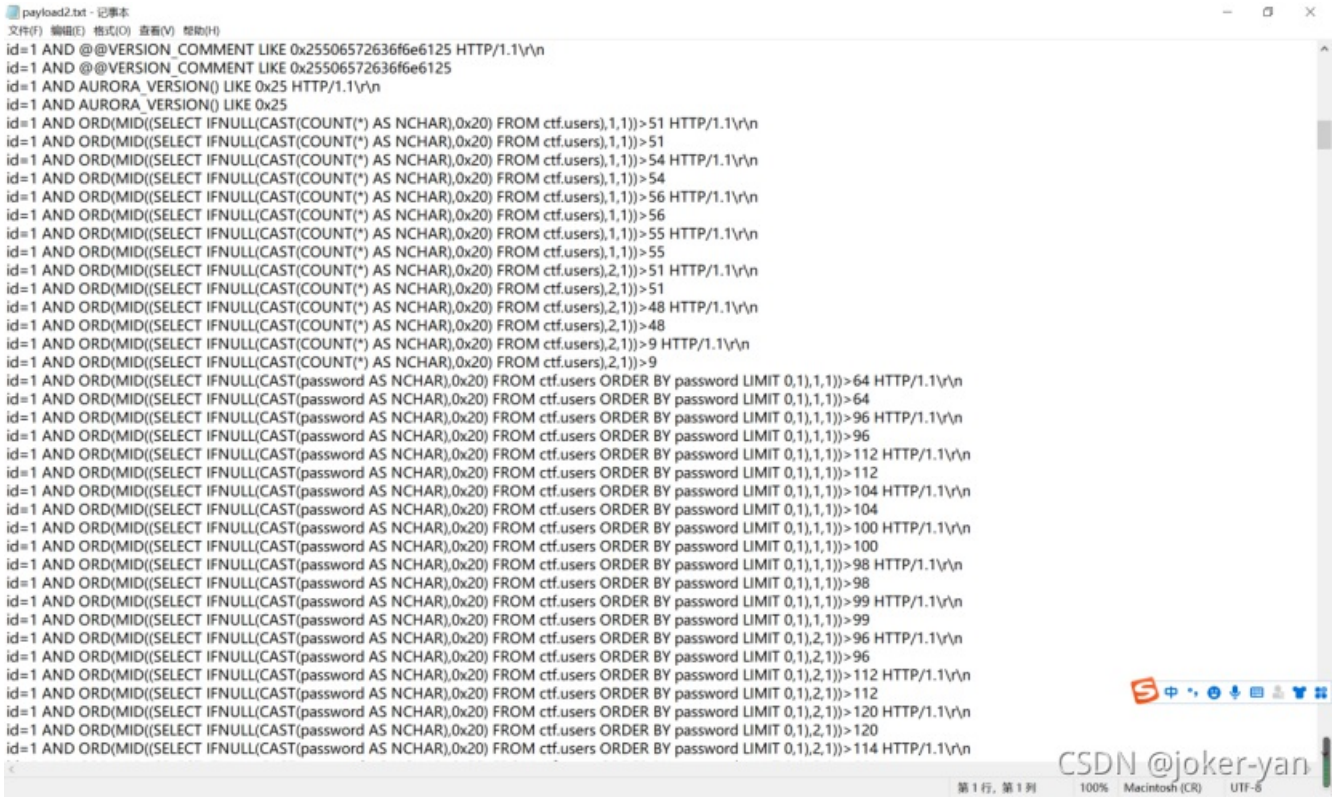
下一步跟踪HTTP流后，



发现存在SQL注入攻击。

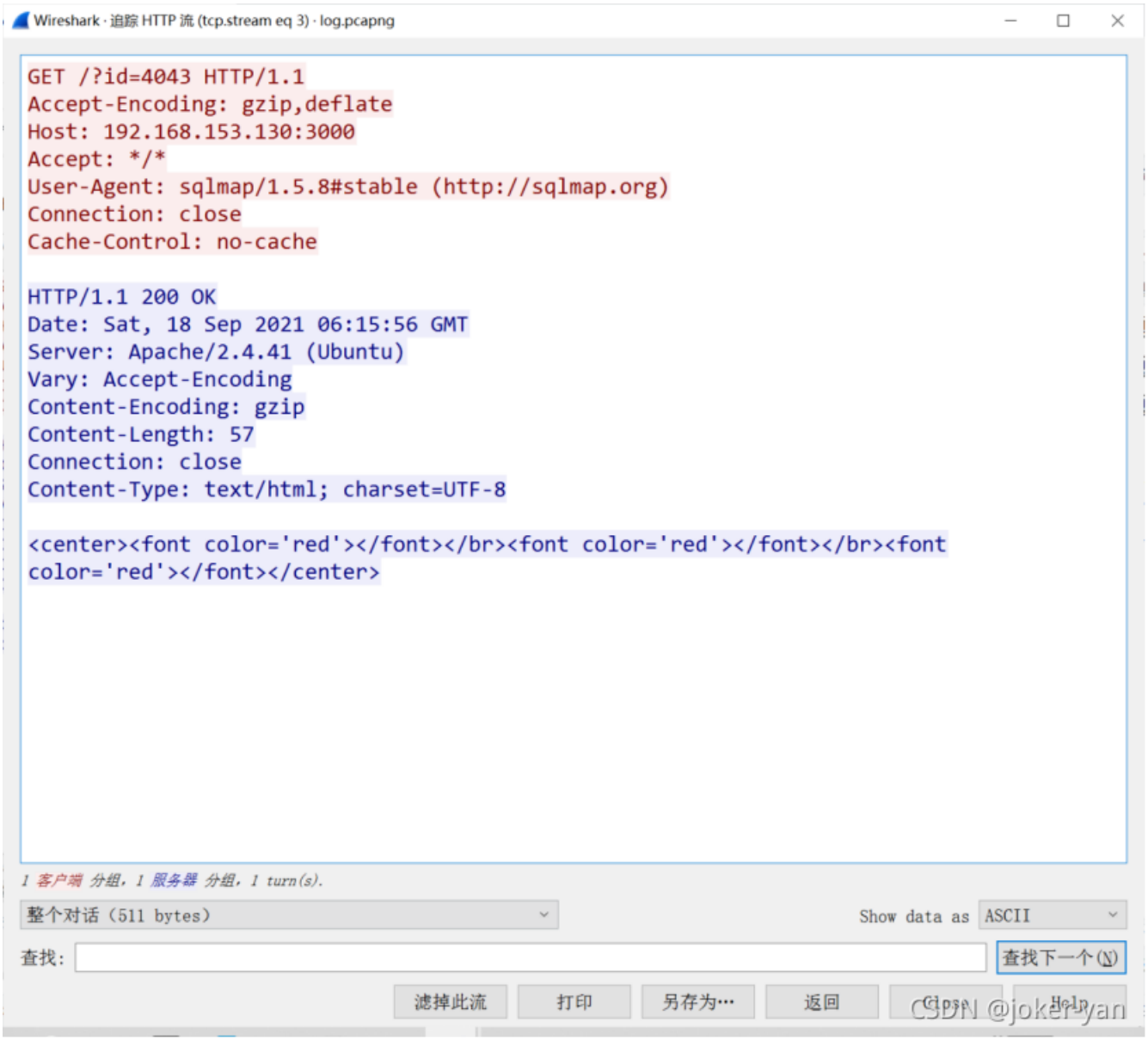
使用python脚本获取传递的参数信息：（附上脚本）

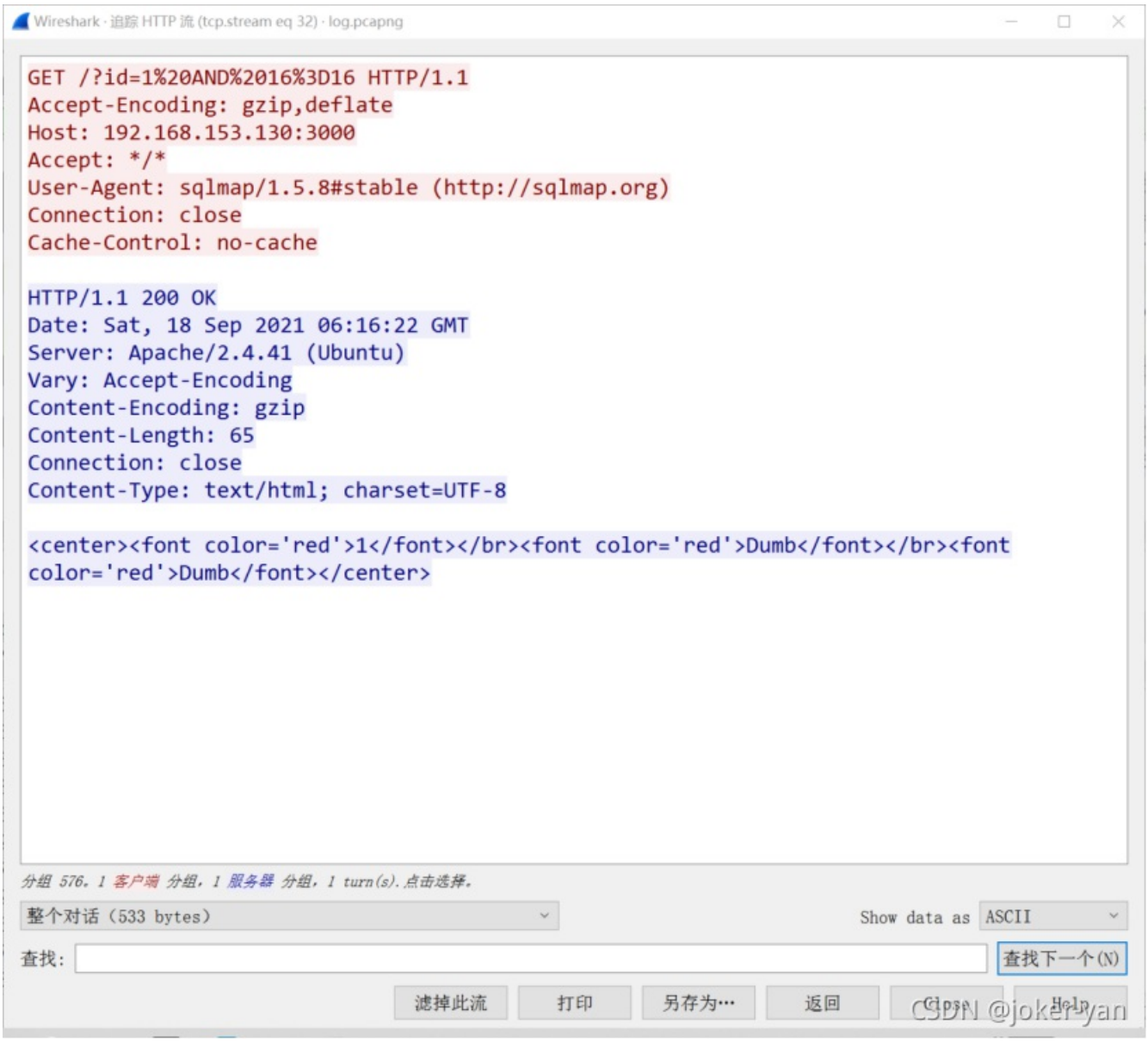
```
import pyshark
import urllib
import re
file=pyshark.FileCapture('log.pcapng',display_filter="http")
#urllib.parse.quote(string)

payload_txt=open('payload2.txt','w+')
txt=''
point=0
flag=''
for i in file:

    string=str(i)
    #print(string,">>>>>")
    string1=re.search( r'id=(.*)', string, re.M|re.I)

    try:
        string1=string1.group()
        string1=urllib.parse.unquote(string1)
    except:
        string1=''

    #print(string)
    if(string1==''):
        pass
    else:
        txt=txt+string1
payload_txt.write(txt)

payload_txt.close()
```



发现存在SQL盲注的痕迹，但是由于判断条件不明朗，所以SQL盲注获取到的信息不明确，

继续跟进，



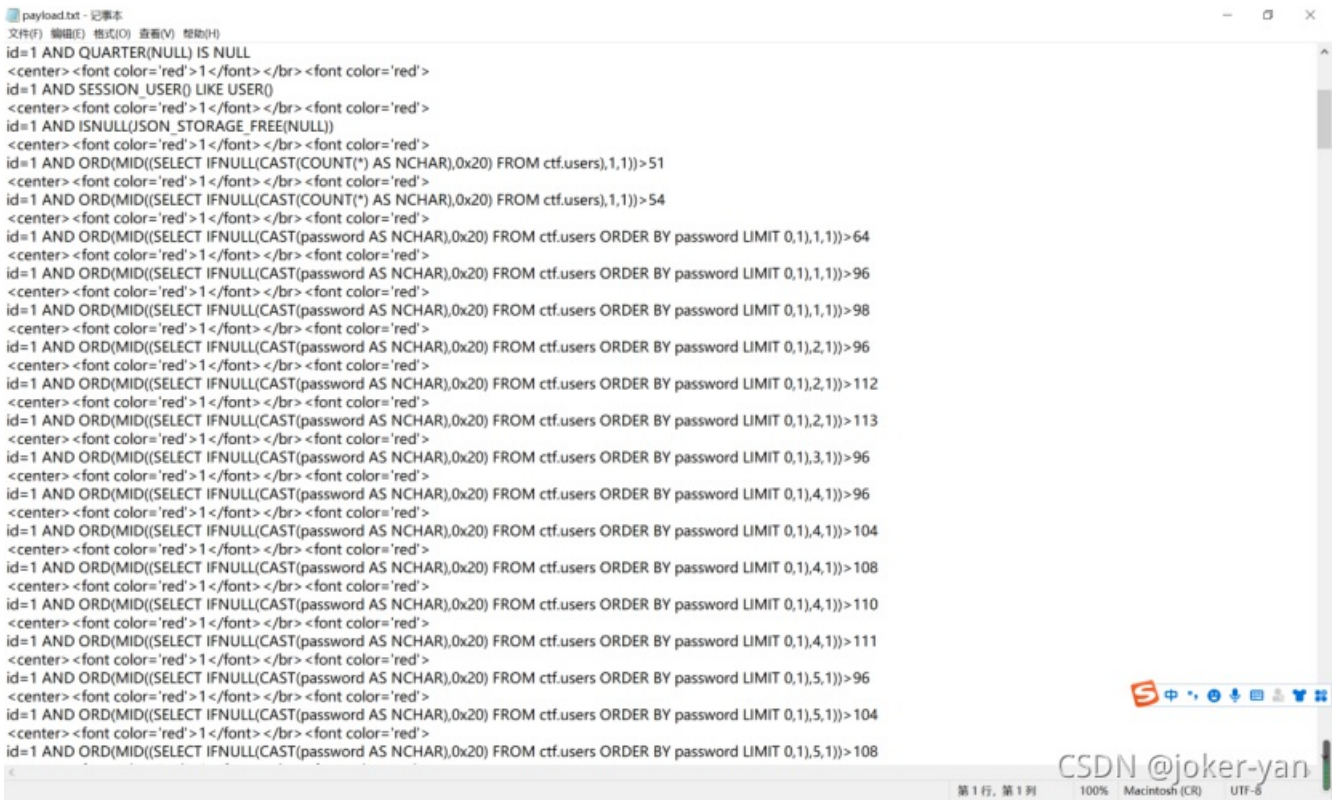


发现有不同的回显，

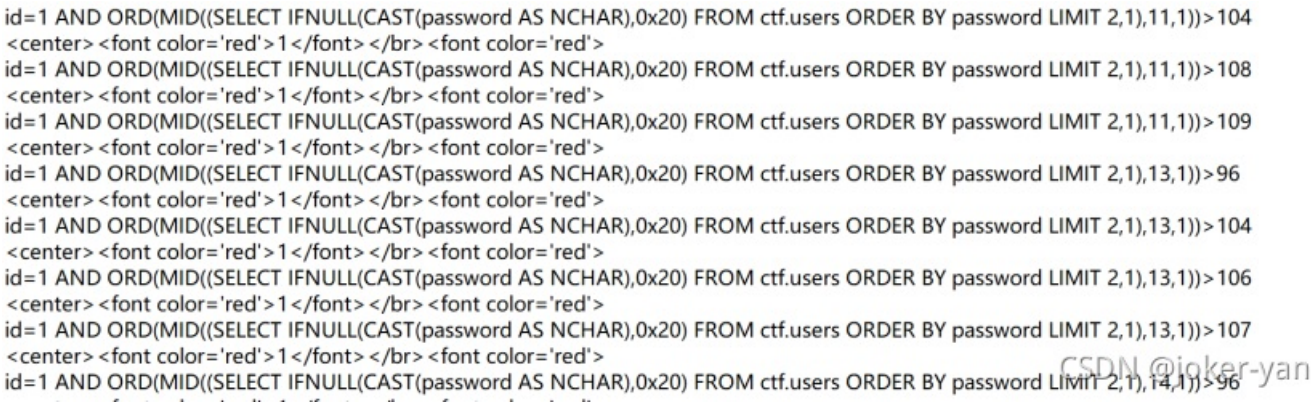
```
<center><font color='red'>1</font></br><font color='red'>Dumb</font></br><font color='red'>Dumb</font></center>
```

更改脚本继续获取数

```
import pyshark
import urllib
import re
file=pyshark.FileCapture('log.pcapng',display_filter="http")
#urllib.parse.quote(string)

payload_txt=open('payload.txt','w+')
txt=''
point=0
flag=''
for i in file:

    string=str(i)
    #print(string,">>>>>")
    string1=re.search( r'id=(.*)', string, re.M|re.I)
    flag=re.search(r"<center><font color='red'>(\d)</font></br><font color='red'>",string,re.M|re.I)
    try:
        if('1'in flag.group()):
            point=1

        else:
            point=0

    except:
        None


    try:
        string1=string1.group()
        string1=urllib.parse.unquote(string1)
        if(point==1):
            string1=string1+flag.group()+'\n'
        else:
            None
    except:
        string1=''


    #print(string)
    if(string1==''):
        pass
    else:
        txt=txt+string1
payload_txt.write(txt)

payload_txt.close()
```



两者对比了一下，发现在“payload.txt”中出现的最后一行数字加上1，再使用python的chr()函数，就是获取到的正确的数字。



缺点在于这里有一个字符没有获取到。

但是获取到了的flag信息是：flag{Log_an?lysis_SQL}

很明显缺少的字符是‘a’

=》flag{Log_analysis_SQL}

总结

“题目很好，队友很强，下次再来~”

这次就弄出来这道题，没想到居然比一血慢了几秒好像QAQ

那道PST文件、内存的题目还是差一点就弄出来了~