




# 平时做题总结

原创

m0re  于 2020-05-09 22:25:05 发布  469  收藏 2

分类专栏: [CTF](#) 文章标签: [CTF writeup](#)

m0re

本文链接: [https://blog.csdn.net/qq\\_45836474/article/details/105628152](https://blog.csdn.net/qq_45836474/article/details/105628152)

版权



[CTF 专栏收录该内容](#)

31 篇文章 3 订阅

订阅专栏

## 本文目录

### Misc

[\[BJDCTF 2nd\]EasyBaBa](#)

[安恒月赛——6G还会远吗](#)

[黄金六年](#)

[\[安淘杯 2019\]吹着贝斯扫二维码](#)

### Crypto

[传统知识+古典密码](#)

[\[NPUCTF2020\]这是什么兔口](#)

[robomunication](#)

[Unencode](#)

### Web

[变量1](#)

[web5](#)

[头等舱](#)

[管理员系统](#)

## Misc

[\[BJDCTF 2nd\]EasyBaBa](#)

## [BJDCTF 2nd]EasyBaBa

## 1

[https://buu-](https://buu-1251267611.file.myqcloud.com/ew3jr3udh39dhendiew/ezbb.jpg)

[1251267611.file.myqcloud.com/ew3jr3udh39dhendiew/ezbb.jpg](https://buu-1251267611.file.myqcloud.com/ew3jr3udh39dhendiew/ezbb.jpg)

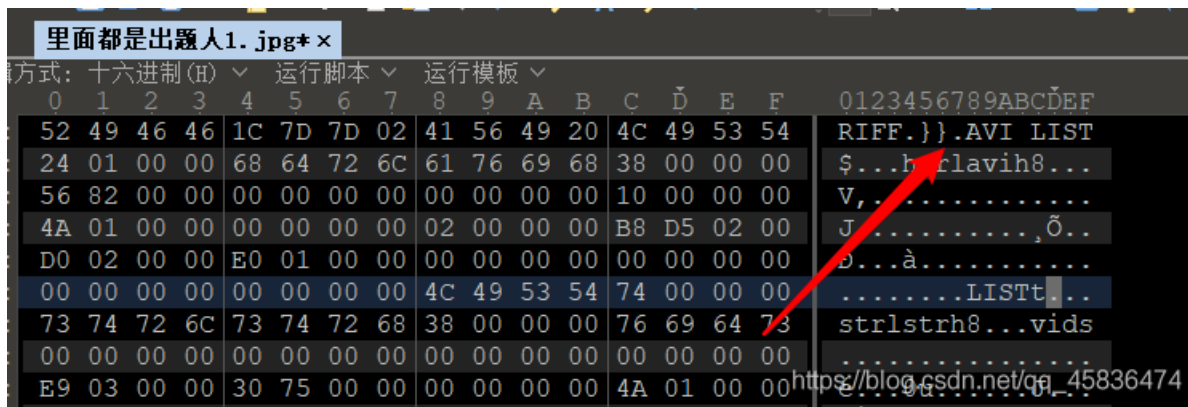
得到的 flag 建议用 flag{} 包上提交。



[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

下载图片后，很大的一张图片，里面必定有东西，foremost分离得到压缩包。

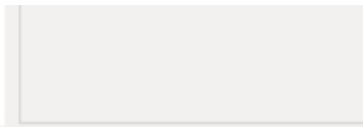
解压后是一张jpg格式的图片，但是打不开，猜想应该可能是文件头缺少，打开010Editor，看一下，发现有点不对劲，



好像是个avi文件，改后缀。打开是一个小视频，好像看过，钉钉来着，全程在叫baba哈。看到中间有几张带二维码的图片闪过去了。太快看不清，用放在PR里逐帧分离，用截图工具Snipaste截取二维码QQ截图也行，（注意截图时，不要截到其他部分，否则修复二维码时会出现解码失败的现象）。

放在扫描工具里修复二维码并扫码





已解码数据 1:

位置:(0.9,-0.3)-(62.6,-0.5)-(1.3,62.5)-(63.0,62.2)

颜色反色,正像

版本:1

纠错等级:L,掩码:2

内容:

316E677D

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

全部扫出来,得到字符串,观察发现符合base16编码的特征。于是进行base16解码

6167696E5F6C6F76655F59424A447B696D316E677D

编码

解码

清空

agin\_love\_YBJD{im1ng}

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

复制

这个答案好奇怪,栅栏也不是啊。难道是什么新的加密?看看比赛时给的wp,

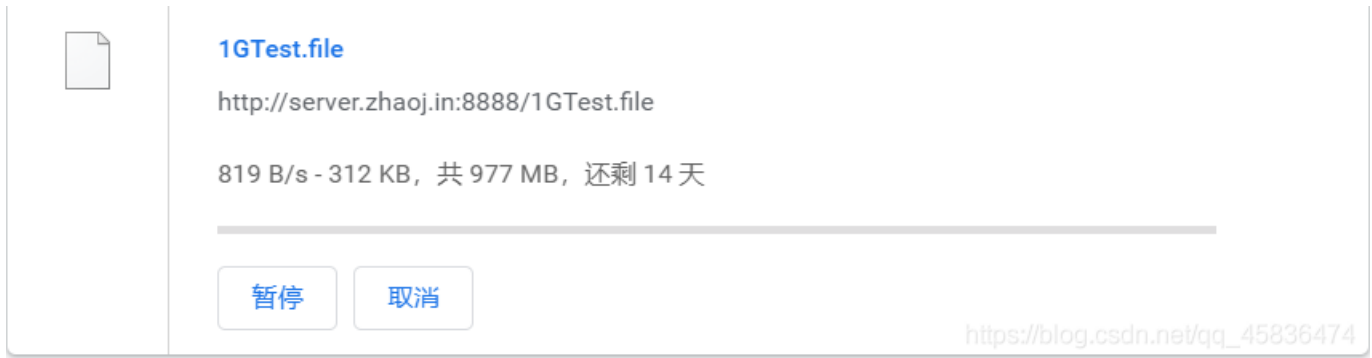
7、(其实这道题是有描述的不知道为什么 buu 通道没了) 可以社工出这是个伪栅栏,调整一下顺序好啦

呃呃呃,是这样吗?????

flag: BJD{imagin\_love\_Y1ng}

安恒月赛——6G还会远吗

题目链接: <http://server.zhaoj.in:8888/1GTest.file>

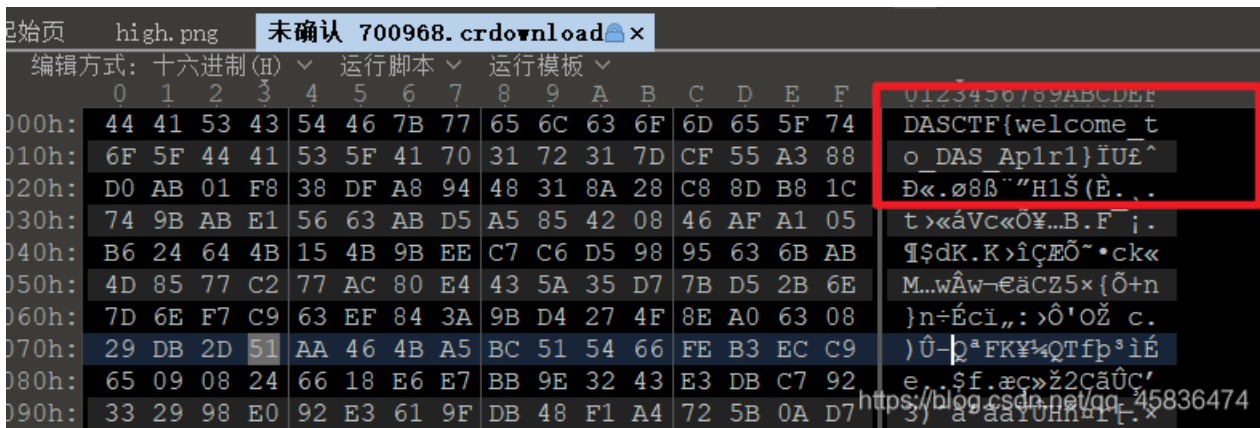


1GTest.file  
<http://server.zhaoj.in:8888/1GTest.file>  
819 B/s - 312 KB, 共 977 MB, 还剩 14 天

暂停 取消

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

14天啊, 是挺无语的, 当时想抓包改什么参数来着, 全都失败。结果看了wp就是直接将没下载完的文件, 放在winhex或010Editor里看。



000h:	010h:	020h:	030h:	040h:	050h:	060h:	070h:	080h:	090h:	0123456789ABCDEF
44 41 53 43	6F 5F 44 41	D0 AB 01 F8	74 9B AB E1	B6 24 64 4B	4D 85 77 C2	7D 6E F7 C9	29 DB 2D 51	65 09 08 24	33 29 98 E0	DASCTF{welcome_t
54 46 7B 77	53 5F 41 70	38 DF A8 94	56 63 AB D5	15 4B 9B EE	77 AC 80 E4	63 EF 84 3A	AA 46 4B A5	66 18 E6 E7	92 E3 61 9F	o_DAS_Ap1r1}IUÉ^
65 6C 63 6F	31 72 31 7D	48 31 8A 28	A5 85 42 08	C7 C6 D5 98	43 5A 35 D7	9B D4 27 4F	BC 51 54 66	BB 9E 32 43	DB 48 F1 A4	Đ«.ø8ß" "H1Š (È. .
6D 65 5F 74	CF 55 A3 88	C8 8D B8 1C	46 AF A1 05	95 63 6B AB	7B D5 2B 6E	8E A0 63 08	FE B3 EC C9	E3 DB C7 92	72 5B 0A D7	t>«áVc«0¥...B.F`i.
										Ŧ\$dK.K>iÇÆÖ~•ck«
										M...wÂw-€äCZ5×{Ö+n
										}n=Éci,,>Ô'OŽ c.
										)Û-p^FK¥¼QTfp³iÉ
										e...sf.ac>ž2CãÜÇ'
										3) a aar0hn1t.x

大写的服!

DASCTF{welcome\_to\_DAS\_Ap1r1}

## 黄金六年

Challenge 115 Solves ×

# [RoarCTF2019]黄金六年

1

得到的 flag 请包上 flag{} 提交。

attachment....

Flag

Submit



复制

Base编码系列: [Base64](#) [Base32](#) [Base16](#)

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

然后大佬们的办法是写脚本，我不会写，只能另外找办法。我就想到将base64编码转换成16进制，然后再保存为rar文件，好像可行。试一下。

UmFyIHoHAQAzkrXICgEFBgAFAQGAADh7ek5VQIDPLAABKEAIEvsUpGAAwAIZmxhZy50eHQwAQAD  
Dx43HyOdLMGWfCE9WEsBZprAJQoBSVIWkJNS9TP5du2kyJ275JzsNo29BnSZCgMC3h+UFV9p1QEf  
JkBPPR6MrYwXmsMCMz67DN/k5u1NYw9ga53a83/B/t2G9FkG/IITuR+9glvr/LEdd1ZRAwUEAA=

Source Type : Text Hex Decoded Result : Hex characters Encoding : UTF-8 Encode Decode

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
52	61	72	21	1A	07	01	00	33	92	B5	E5	0A	01	05	06
00	05	01	01	80	80	00	E1	ED	E9	39	55	02	03	3C	B0
00	04	A1	00	20	4B	EC	52	91	80	03	00	08	66	6C	61
67	2E	74	78	74	30	01	00	03	0F	1E	37	1F	23	9D	2C
C1	96	7C	21	3D	58	4B	01	66	9A	C0	25	0A	01	49	59
56	90	93	52	F5	33	F9	76	ED	A4	C8	9D	BB	E4	9C	EC
36	8D	BD	06	74	99	0A	03	02	DE	1F	94	15	5F	69	D5
01	1F	26	40	4F	3D	1E	8C	AD	8C	17	9A	C3	02	33	3E

网站地址: [base64转换成16进制](#)

然后，复制十六进制的编码粘贴到HxD中进行保存。

Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000 52 61 72 21 1A 07 01 00 33 92 B5 E5 0A 01 05 06 Rar!....3'µå....  
00000010 00 05 01 01 80 80 00 E1 ED E9 39 55 02 03 3C B0 ....€€.áíé9U..<°  
00000020 00 04 A1 00 20 4B EC 52 91 80 03 00 08 66 6C 61 ..;. KìR'€...fla  
00000030 67 2E 74 78 74 30 01 00 03 0F 1E 37 1F 23 9D 2C g.txt0.....7.#.,  
00000040 C1 96 7C 21 3D 58 4B 01 66 9A C0 25 0A 01 49 59 Á-|!=XK.fšÀ%..IY  
00000050 56 90 93 52 F5 33 F9 76 ED A4 C8 9D BB E4 9C EC V."Rõ3ùvívÈ.»æèì  
00000060 36 8D BD 06 74 99 0A 03 02 DE 1F 94 15 5F 69 D5 6.¿.t™...P.". iÖ  
00000070 01 1F 26 40 4F 3D 1E 8C AD 8C 17 9A C3 02 33 3E ..&@O=.€.(.šÄ.3>  
00000080 BB 0C DF E4 E6 ED 4D 63 0F 60 6B 9D DA F3 7F C1 ».BäæiMc.`k.Úó.Á  
00000090 FE DD 86 F4 59 06 FC 82 13 B9 1F BD 80 8B EB FC pÝtôY.ü.,¿€<ëü  
000000A0 B1 1D 77 56 51 03 05 04 00 ±.wVQ....[]

保存后，打开看看，果然能打开，加密的，密码就是前面得到的那个字符串，解压得到flag

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

```
flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
roarctf{CTF-from-RuMen-to-RuYuan}
```

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

提交正确。

## [安洵杯 2019]吹着贝斯扫二维码

Challenge 102 Solves ×

# [安洵杯 2019]吹着贝斯扫二维码

1

得到的 flag 请包上 flag{} 提交。



Flag

Submit

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

解压发现一堆文件

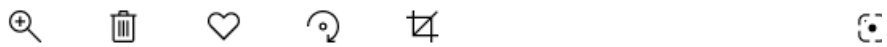
名称	修改日期	类型
6lk34u72te5s79kzj0dr	2019/11/6 1:16	文件
6q13s096tu512c8f7z8x	2019/11/6 1:16	文件
7vh669w0zagz936z28h5	2019/11/6 1:16	文件
09w91x992i4ijx6iq27	2019/11/6 1:16	文件
9g896pxvd013rx16r0xf	2019/11/6 1:16	文件
14c6p1j84uis3453298a	2019/11/6 1:16	文件
64g80t29b7kjh8nxoiu	2019/11/6 1:16	文件
67pt042zw26y3e350i4s	2019/11/6 1:16	文件
88u9ofh6oud8lx62r1h3	2019/11/6 1:16	文件
227j301wb8cq7l29qf9y	2019/11/6 1:16	文件
284rgt186c76v758xpc7	2019/11/6 1:16	文件
576lit819036i9i31s45	2019/11/6 1:16	文件



1453k669k20puqnxjwrb	2019/11/6 1:16	文件
8151ltvll69t7n8dqd18	2019/11/6 1:16	文件
66068yso21h7m48kmjyr	2019/11/6 1:16	文件
448931j6ihj30h4v7llv	2019/11/6 1:16	文件
649882lp5734tuu48of2	2019/11/6 1:16	文件
ag32l406e0h957h	2019/11/6 1:16	文件
bj245p444s05lfx	2019/11/6 1:16	文件
flag.zip	2019/11/6 1:14	WinI
gu4c2ce0t7558a2lepos	2019/11/6 1:16	文件
l5e87tbyb7n1q5l91yp0	2019/11/6 1:16	文件
m2h25uf40kr28l08n4a6	2019/11/6 1:16	文件

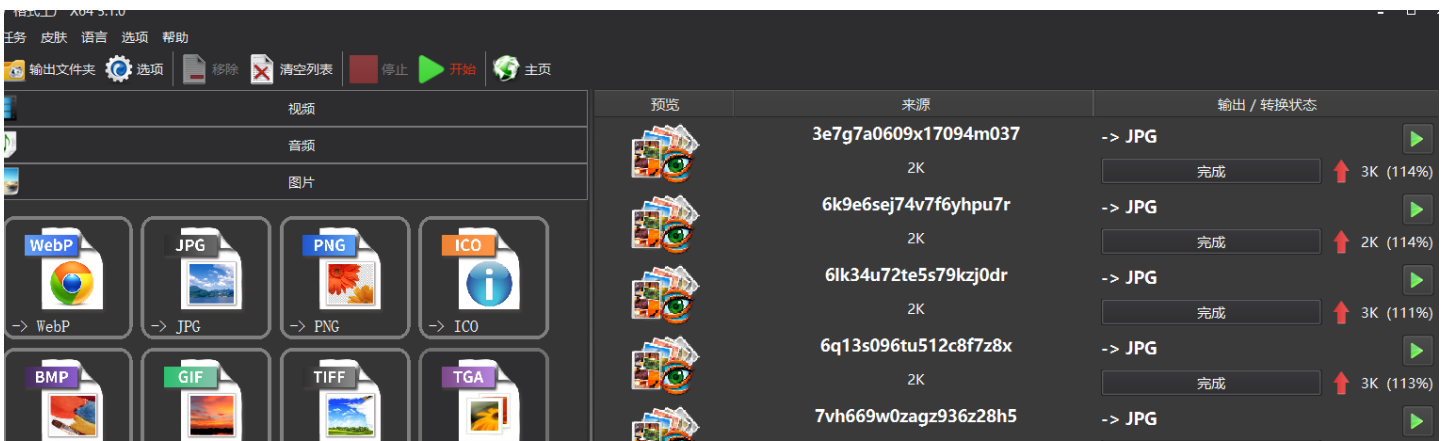
类型: 文件  
大小: 2.55 KB  
修改日期: 2019/11/6 1:16

而且压缩包还是加密的，看看那些文件，发现都有JPEG，可能是jpg图片，先改一个看看。

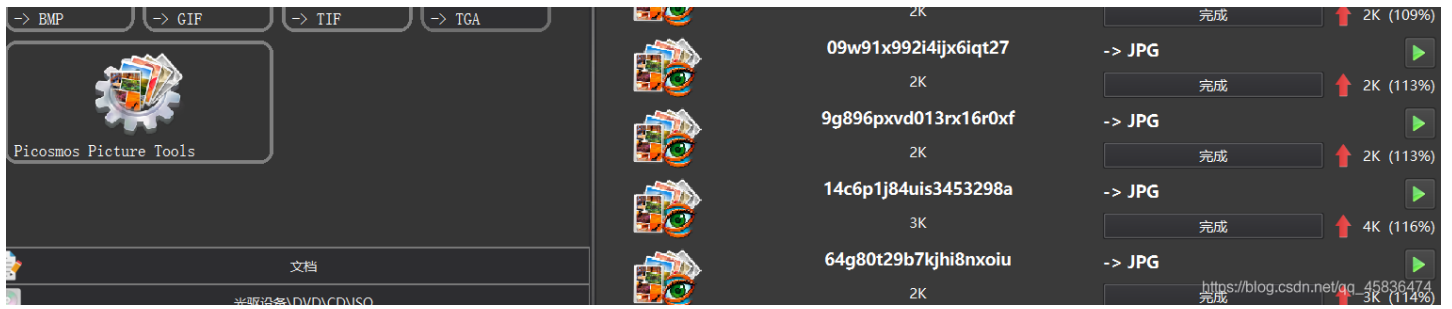


[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

有点东西，总不能一个一个改吧？这么多，然后在百度的小角落里发现了一个工具——格式工厂(最喜欢工具了)







真快，看一下。



好家伙，拼图。得到36张图，可以拼一张6x6的大图。

将文件夹拖进kali。然后使用工具拼图。

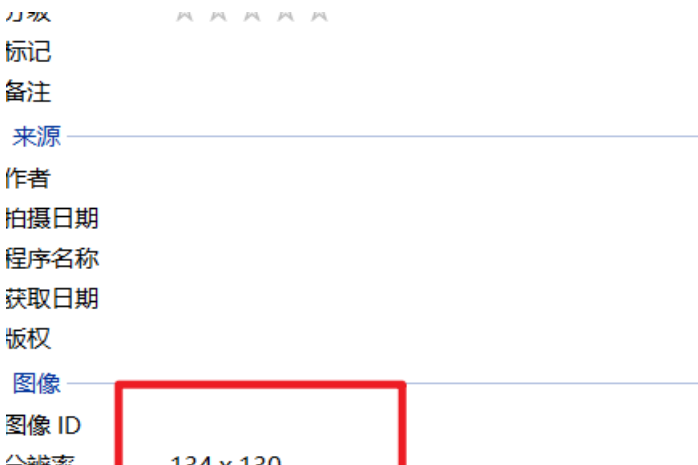
在文件夹内打开终端

```
montage *.jpg -tile 6x6 -geometry 134x130+0+0 out.jpg
```

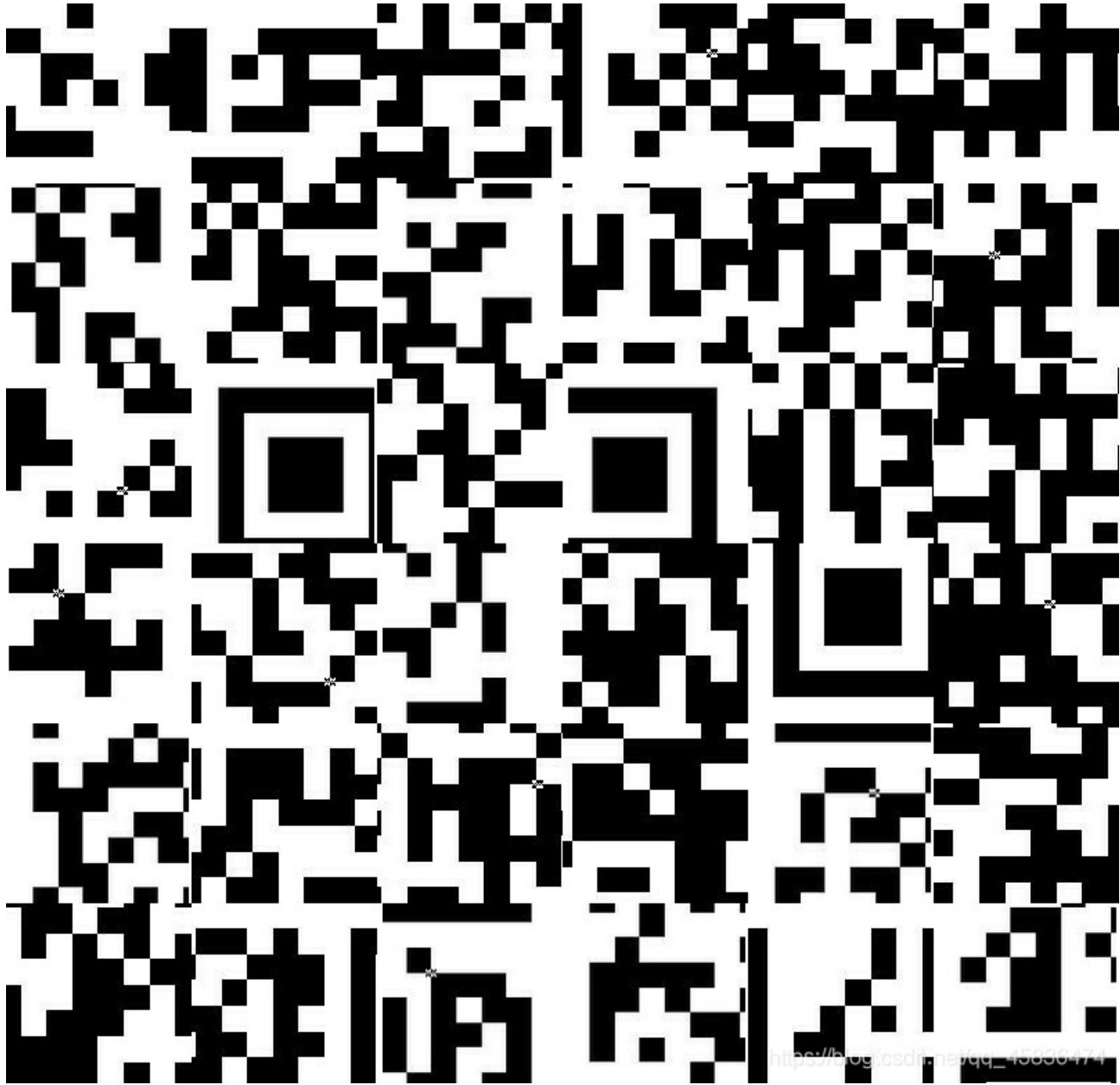
然后得到一张混乱无序的图。

注意这里的像素：要和分裂的二维码残片的像素一致才能得出这样的二维码乱序图。如果像素不一样了，就得不到这样的图，当然后面的步骤也就无法进行下去。

而这张图的像素：打开一张二维码片段，然后看它的属性里面——详细信息



分辨率	134 x 130
宽度	134 像素
高度	130 像素
水平分辨率	96 dpi
垂直分辨率	96 dpi
位深度	24
压缩	<a href="https://blog.csdn.net/qq_45836474">https://blog.csdn.net/qq_45836474</a>

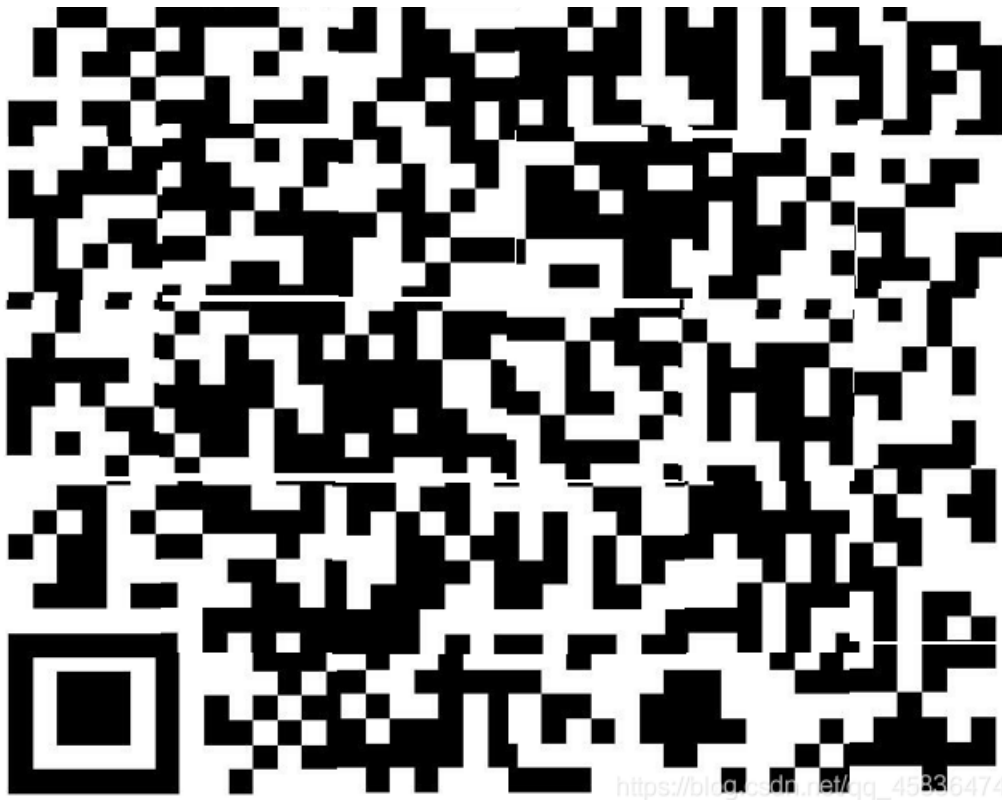


再使用gaps还原

```
gaps --image=out.jpg --generations=40 --population=36 --size=100
```

没还原出来，尴尬哈，，，不知道怎么回事，我试了n次了，就是还原不出来。奇怪了。最后我实在是没办法了，只上手了。在PPT里拼的。md 累死，我拼了俩小时(泪流满面.gif)





[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

扫描吧，终于可以扫了。

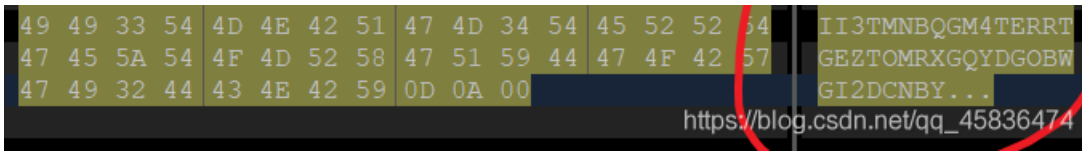
已解码数据 1:

位置:(14.2,9.7)-(635.5,11.1)-(14.0,618.8)-(635.9,621.7)  
颜色正常,正像  
版本:6  
纠错等级:H,掩码:3  
内容:  
BASE Family Bucket ??? 85->64->85->13->16->32

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

emmm，啥玩意儿。好像还有个flag.zip没看。

attachment.zip																flag.zip x															
方式: 十六进制(H) v 运行脚本 v 运行模板: ZIP.bt v D																															
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
50	4B	03	04	14	00	01	00	00	00	12	08	66	4F	7B	2C	PK.....fO{,															
B1	B4	22	00	00	00	16	00	00	00	08	00	00	00	66	6C	±'.....fl															
61	67	2E	74	78	74	29	F8	82	0C	18	4C	30	3E	A8	DF	ag.txt)ø,..L0>"ß															
AE	AE	9A	C6	81	17	58	C9	91	5B	E0	A5	3C	90	56	26	ööšÆ..XÉ`[à¥<.V&															
3B	AB	C2	CA	28	BE	3D	01	50	4B	01	02	3F	00	14	00	;«ÂÊ(¾=.PK..?...															
01	00	00	00	12	08	66	4F	7B	2C	B1	B4	22	00	00	00	.....fO{,±'...															
16	00	00	00	08	00	24	00	00	00	00	00	00	00	20	08	.....ş.....															
00	00	00	00	00	00	66	6C	61	67	2E	74	78	74	0A	00	.....flag.txt..															
20	00	00	00	00	00	01	00	18	00	D1	99	A8	8A	FA	93	.....Ñ™"Šú"															
D5	01	47	B1	B3	F4	F9	93	D5	01	47	B1	B3	F4	F9	93	Ń.G±³ou Ń.G±³òù"															
D5	01	50	4B	05	06	00	00	00	00	01	00	01	00	5A	00	Ń.PK.....Z.															
00	00	48	00	00	00	73	00	47	4E	41	54	4F	4D	4A	56	..H...s.GNATOMJ															
49	51	5A	55	4B	4E	4A	58	47	52	43	54	47	4E	52	54	IQZUKNJXGRCTGNRT															
47	49	33	45	4D	4E	5A	54	47	4E	42	54	4B	52	4A	57	GI3EMNZTGNBTKRJW															
47	49	32	55	49	4D	52	52	47	4E	42	44	45	51	5A	57	GI2UIMRRGNBDEQZW															
47	49	33	44	4B	4D	53	46	47	4E	43	44	4D	52	4A	54	GI3DKMSFGNCDMRJT															



嗷嗷，还有编码。复制出来解密。

上面扫出来的好像是加密顺序，因为题目中的二维码已经扫过了，还有贝斯。那应该是base编码。

这个编码好像是base32 编码，那就是解密过程，上面的是加密顺序，将它逆转一下。开始解码。

这题真的给我解吐了。转过来转过去。

得到压缩包密码，ThisIsSecret!233

解压flag.zip得到

```
flag{Qr_Is_MeAn1nGfuL}
```

这一道题真是耗费我好长时间。

## Crypto

### 传统知识+古典密码

Challenge 350 Solves

# 传统知识+古典密码

## 1

注意：得到的 flag 请包上 flag{} 提交

Download: d6f96e23-1f...

Flag Submit

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

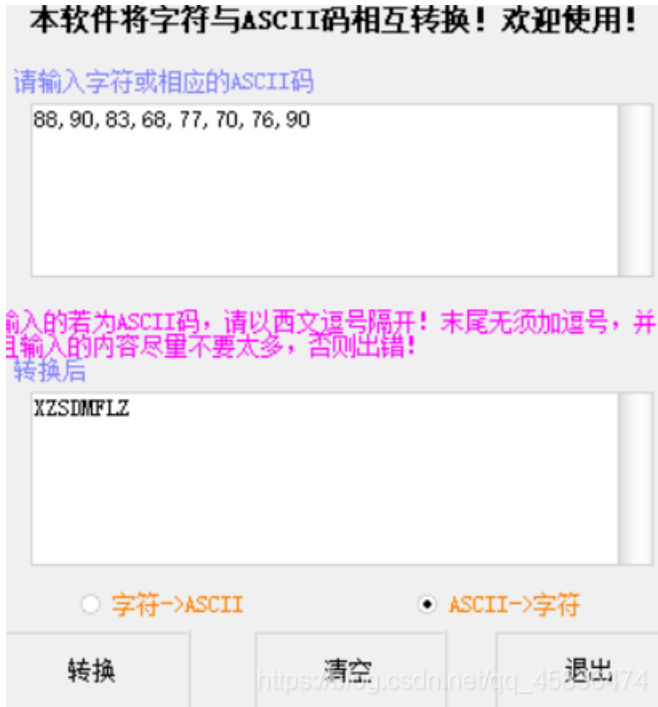
看着是年份，还是六十甲子年份。应该是要换成数字。于是百度对照表。把数字对照出来。而且背面还写了 +甲子 再加上60。一甲子是六十

小明某一天收到一封密信，信中写了几个不同的年份  
辛卯，癸巳，丙戌，辛未，庚辰，癸酉，己卯，癸巳。  
信的背面还写有“+甲子”，请解出这段密文。

key值: CTF{XXX}

辛卯	癸巳	丙戌	辛未	庚辰	癸酉	己卯	癸巳
28	30	23	8	17	10	16	30
88	90	83	68	77	70	76	90

第一想法应该是ASCII码表。对照出来。



然后看着这一串字符，没了头绪。再看看题，没有提示了啊。然后发现一个重要的事，题目说传统密码加古典密码。我好像没用到古典密码啊。脑中快速过了一遍古典密码。这么短的字符串，应该是凯撒密码，还有栅栏密码，其他的一下子没想太多。八个字符，栅栏可以分两栏和四栏，试过之后是两栏的。



然后凯撒解密。

得到

XMZFSLDZ

位移

加密

解密

SHUANGYU

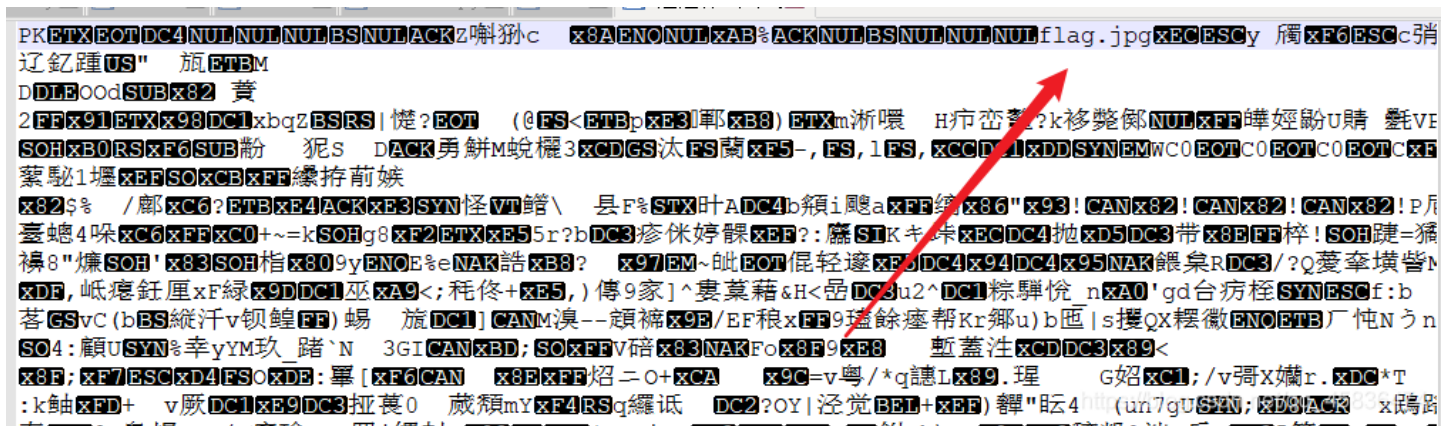
[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

至于是偏移5位，自己一个一个试出来的，就这个最靠谱。

[\[NPUCTF2020\]这是什么觅](#) □

这个比赛我也看了，当时就看这一道题能看出来点门道，当然我一道题都没做出来，没什么可丢人的。就把这道题复现一下。也是成长过程。

下载得到一个文件，刚开始没有思路啊，没有想太多，不知道用什么方法打开，就直接payload++打开看了一眼，然后发现了



然后，foremost分离文件，得到了压缩包。



这个我没想到有什么古典密码是这个的，然后看着右下角的纸条，这种有空隙的，是不是键盘密码之类的，再仔细想想不对，放弃，后来看着上面的日历，在这里面找，没啥头绪。再回头看那串字符串。发现第一个字母都是大些且 F、W、S、S、T、S、W、S 有个规律就是他们英文单词星期的首字母。这个一想就靠谱，就抓住这一点来想。后面跟数字，再看日历，第一排画圈了。没错的，就是这样，字母后面跟两个数字的都是在一周中又重复出现的。所以第一个字母是他们的顺序。第二个字母才是出题人想给的信息。这样看出来就是

3 1 12 5 14 4 1 18，我不知道为什么把1算上了，不是已经划了吗？

不过不纠结这个，我到这里卡住了。所以后面的看的师傅们的博客知道的。然后发现字母表的，我之前一直在猜ascii码，就这个没想到。所以一道题没做出来。最后 `flag{calendar}`

robomunication





Challenge

114 Solves



# Unencode

1

注意：得到的 flag 请包上 flag{} 提交

 e414b69a-5...

Flag

Submit

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

什么提示都没有，，就一串编码，而且看着怎么也不想不起来什么密码是这样的，见识短浅了。

是UUencode编码

直接在线网站解就行了。

[UUencode在线解码](#)

flag{dsdasdsa99877LLLLKK}

## Web

web题先从简单的来，不然太容易被搞乱心态。

### 变量1

Challenge

10418 Solves



变量1  
60

<http://123.206.87.240:8004/index1.php>

Flag

Submit

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

代码审计:

```
flag In the variable ! <?php
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/", $args)){
        die("args error!");
    }
    eval("var_dump($$args);");
}
?>
```

首先注意到的是正则表达式, 关于正则表达式的学习, 在学习PHP时了解过了, 这个是要匹配正确的字符串。

`\w` 匹配任意一个数字或字母或下划线

如果不匹配则直接die, 匹配的话就输出一个可变量, 重点就在可变量这里。我刚开始进行尝试, 构造 `?args=_lala_` 结果输出了NULL, 好像与eval函数有关, 发现对eval函数了解的不够, 就又查了一遍。

## 定义和用法

`eval()` 函数把字符串按照 PHP 代码来计算。

该字符串必须是合法的 PHP 代码, 且必须以分号结尾。

如果没有在代码字符串中调用 `return` 语句, 则返回 NULL。如果代码中存在解析错误, 则 `eval()` 函数返回 `false`。

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)

`$$args` 代表一个变量, 所以这里传一个全局变量给它, 全局变量有九种, 可以挨个试, 九大全局变量在百度直接搜索就可以搜到。

- 1| \$\_POST [用于接收post提交的数据]
- 2| \$\_GET [用于获取url地址栏的参数数据]
- 3| \$\_FILES [用于文件接收的处理img 最常见]
- 4| \$\_COOKIE [用于获取与setCookie()中的name 值]
- 5| \$\_SESSION [用于存储session的值或获取session中的值]
- 6| \$\_REQUEST [具有get,post的功能, 但比较慢]
- 7| SERVER [是预定义服务器变量的一种, 所有SERVER[是预定义服务器变量的一种, 所有\_SERVER [是预定义服务器变量的一种, 所有\_SERVER开头的都
- 8| \$GLOBALS [一个包含了全部变量的全局组合数组]
- 9| \$\_ENV [是一个包含服务器端环境变量的数组。它是PHP中一个超级全局变量, 我们可以在PHP 程序的任何地方直接访问它]

然后, 用到了GLOBALS就得到了flag

```

flag in the variable ! <?php
error_reporting(0);
include "flag1.php";
highlight_file(__FILE__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^w+$/", $args)){
        die("args error!");
    }
    eval("var_dump($args);");
}
array(7) { ["GLOBALS"]=> *RECURSION* ["_POST"]=> array(0) {} ["_GET"]=> array(1) { ["args"]=> string(7) "GLOBALS" } ["_COOKIE"]=> array(0) {} ["_FILES"]=> array(0) {} ["ZFkwe3"]=> string(38) "flag(92853051ab894a64f7865cf3c2128b34)" ["args"]=> string(7) "GLOBALS" }

```

## web5

f12发现了非常多的编码, 查百度, 发现是jother编码, 而且控制台可解。直接复制所有编码粘贴到控制台, 回车即可。flag大写。

## 头等舱

打开网页什么也没有, 没有其他提示, 回头看题目, “头”等舱。header。进行抓包尝试。成功找到flag

## 管理员系统

f12查看有无有用信息, 找到一个base64编码(==), 解码得到test123, 应该是密码了吧。

所以尝试登陆: 发现登录失败, 而且IP禁止访问, 联系本地管理员。

所以可能是XFF。可以改一下, 本地管理员那就改成本地的127.0.0.1

可以抓包添加, 我直接使用chrome扩展插件添加了, 然后刷新网页, 得到flag。

# 管理员系统

Username:

Password:

**The flag is: 85ff2ee4171396724bae20c0bd851f6b**

[https://blog.csdn.net/qq\\_45836474](https://blog.csdn.net/qq_45836474)