

实验吧安全杂项WP（二）

原创

Neil-Yale 于 2017-03-20 12:20:47 发布 3925 收藏 2

文章标签: [python](#) [安全](#) [二进制](#) [ascii](#) [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/yalecaltech/article/details/64124021>

版权

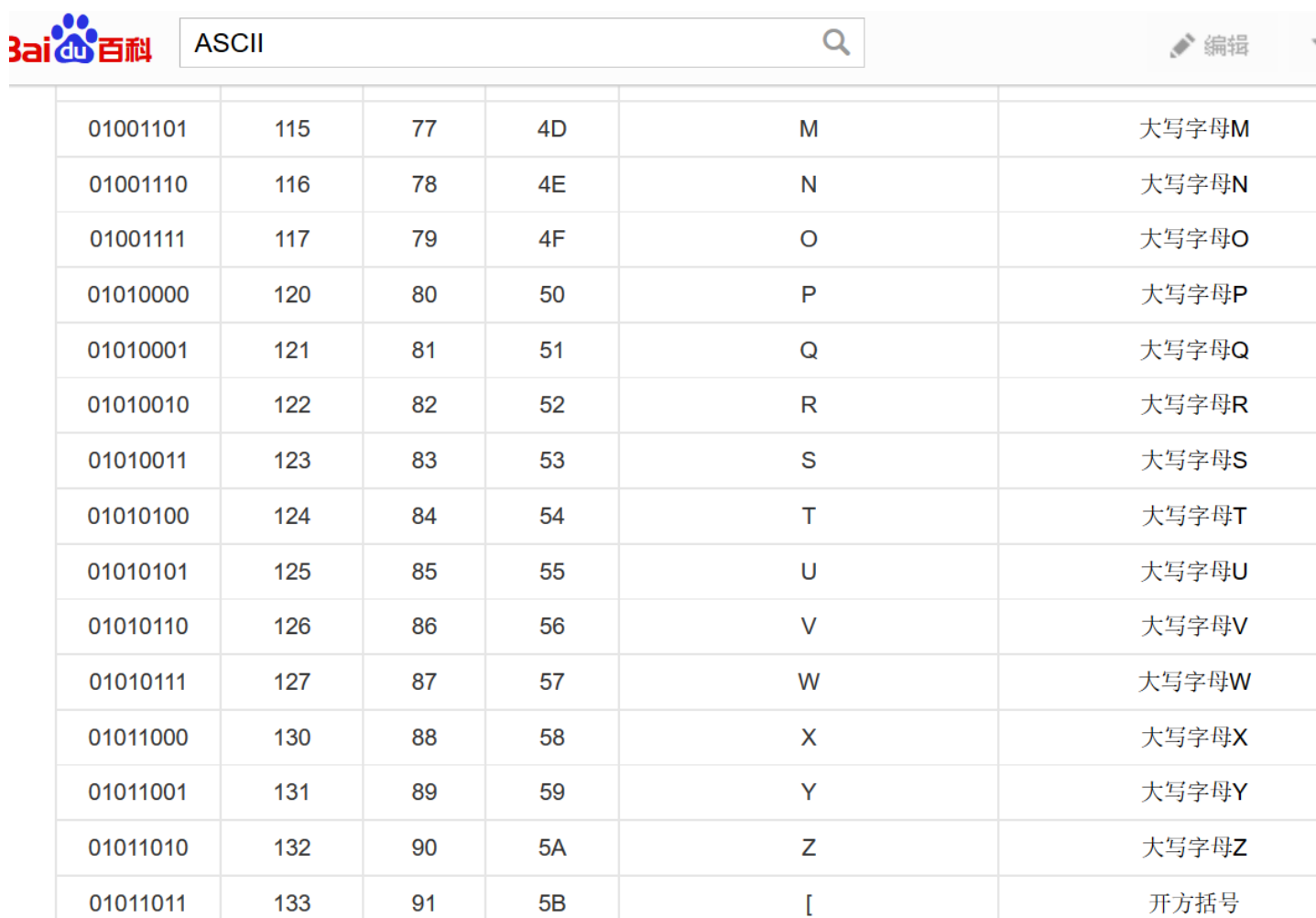
1. 解码磁带 (<http://www.shiyanbar.com/ctf/1891>)

只有字符'o'和下划线', 不免让我们想起二进制, 只有0和1, 却能表示所有信息, 所以我们尝试用0, 1替换o和

而究竟0对于o还是_呢? 我们有例子可以得到

跑python的思路是这样子的, 换成二进制后再转换成ascii, 然后相应解码即可, 也可以参考这张图片

直接用二进制对应字母



01001101	115	77	4D	M	大写字母M
01001110	116	78	4E	N	大写字母N
01001111	117	79	4F	O	大写字母O
01010000	120	80	50	P	大写字母P
01010001	121	81	51	Q	大写字母Q
01010010	122	82	52	R	大写字母R
01010011	123	83	53	S	大写字母S
01010100	124	84	54	T	大写字母T
01010101	125	85	55	U	大写字母U
01010110	126	86	56	V	大写字母V
01010111	127	87	57	W	大写字母W
01011000	130	88	58	X	大写字母X
01011001	131	89	59	Y	大写字母Y
01011010	132	90	5A	Z	大写字母Z
01011011	133	91	5B	[开方括号

python结果如下:

```
1.py x
1 f=open('1.txt','r')
2 line=f.readline().strip('\n')
3 s=str()
4 while line:
5     number=int(line,2)
6     char=chr(number)
```

```

7 s+=char
8 line=f.readline().strip('\n')
9 print (s)

```

Run 1

C:\Python27\python.exe C:/Users/hasee/Desktop/Pythor
Where there is a will,there is a way.

按照格式提交即可

2.功夫秘籍 (<http://www.shiyanbar.com/ctf/1887>)

下载来的是一个压缩包，打开它。。。我的天，居然打不开。扔到winhex看看，发现是png

kungfu.rar															
3	4	5	6	7	8	9	A	B	C	D	E	F			
17	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	!	PNG	IHDR
18	00	00	00	DD	08	02	00	00	00	07	12	8D	ä	Ý	
19	03	73	42	49	54	08	08	08	DB	E1	4F	E0	s	BIT	Úá0à
20	70	48	59	73	00	00	0E	C4	00	00	0E	C4	p	HYS	Ä Ä
21	1B	00	00	20	00	49	44	41	54	78	9C	9C	!	+	IDATx!!
22	49	72	24	C8	2C	A2	6A	E6	11	91	59	AF	¸	['\$Ir\$È,çjæ 'Y
23	0C	06	83	05	40	0B	D0	D2	EC	D7	DC	66	.	ó	h ! @ ð0i×Üf
24	B5	87	D9	B3	00	68	34	2A	33	E3	E1	6E	ÿ	æk	µ!Û° h4*3áán
25	B	21	E6	1E	9E	D5	D5	43	4B	B0	8E	2E	8A		*Áú!æ !ÖÖCK°!.
26	57	13	65	61	61	79	38	FF	E3	79	FF	9F	ó	°°0W	eaay8ÿäÿÿ!
27	AD	F5	DE	7B	EF	EE	4E	12	80	24	FC	F2	ÿ	×ÿl-ðp{iiN !\$üò	
28	29	80	24	09	4E	CD	48	0D	E5	94	66	44	!	âEH)!\$	NÍH á!fD
29	F6	71	19	63	8F	08	03	33	33	46	64	26	Ï	,	Ä>öq c 33Fd&
30	CC	CC	3D	A6	F7	06	D9	25	46	64	C2	0D	"	3s!í!i=!	÷ Û%FdÄ
31	70	31	5F	AD	7D	EC	EB	43	5F	3F	B6	75	t	I!	2p1_-}ièC_?¶u
32	F8	F8	F8	B4	3C	9C	12	02	B0	3E	3E	9C	ð	öxzøøø`<!	°>>!

本来想直接改成png的，但是想到改了之后还是要winhex,干脆直接搜索key,flag等关键字，找到了

J22260	00	00	00	00	49	45	4E	44	AE	42	60	82	6B	65	79	20	I	END@B`!key
J22270	69	73	20	56	46	39	35	63	30	73	35	58	7A	56	79	61	i	s VF95c0s5XzVya
J22280	47	74	66	58	33	56	47	54	58	52	39	4D	30	56	73	65	G	tfX3VGTXR9M0Vse
J22290	32	35	31	51	45	55	67	20	20								2	51QEUG

目测base64，解码

```

VF95c0s5XzVyaGtfX3VGTXR9M0Vse251QEUG

```

解码结果以16进制显示

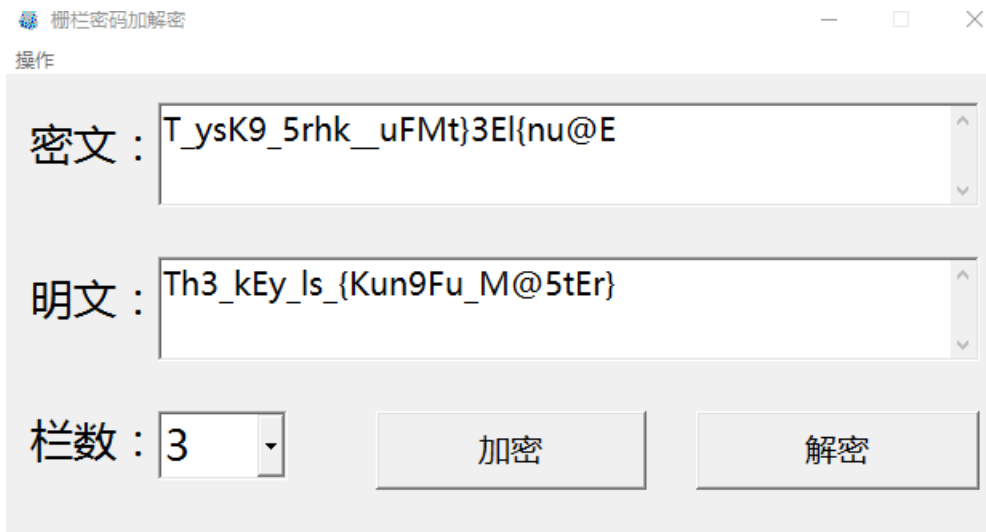
Base64编码或解码结果：

```

T_ysK9_5rhk_uFMt}3E1{nu@E

```

目测栅栏，解码



提交时只需要提交{}里面的内容就行了

3.WTF? (<http://www.shiyanbar.com/ctf/1886>)

打开一看一堆乱七八糟的东西，不过拉到最下面发现有=，base64解之
得到01的组合

数了一下有65536 = 256*256

正方形是吧

那么尝试组个正方形出来

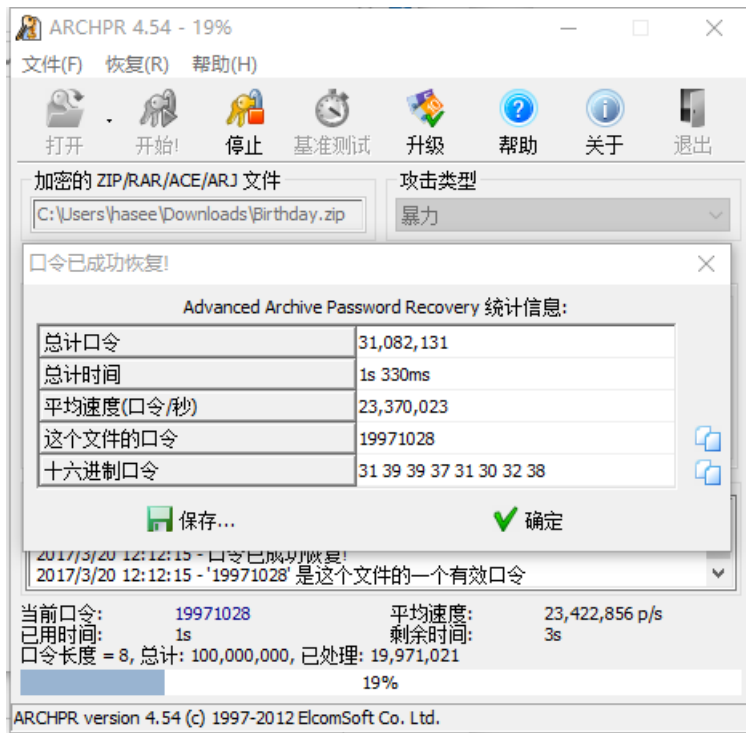
作图的话processing挺好用



扫一扫就出来了

4. 社交网络 (<http://www.shiyanbar.com/ctf/1879>)

下载来的压缩文件需要密码，爆破之



解压后得到文件，右键查看属性，得到flag

5.想知道Key只有一个办法(<http://www.shiyanbar.com/ctf/1863>)

无话可说

- 1、加入QQ粉丝群 (384182110) ;
- 2、询问传说哥微信号 ;
- 3、微信找传说哥要Key ;
- 4、他的微信不定期有惊喜。

解题链接：**通过**

CTF{chuanshuoge_bigboss}

评论

请遵守实验吧相关发言规则，切勿在评论、文章中发表不适当的言论



pcats

鉴于各种原因，我直接贴flag。CTF{chuanshuoge_bigboss}

<http://blog.csdn.net/yalecaltech>

好人一生平安