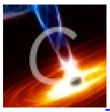
N1CTF 2018 lipstick WriteUp (bugku——多彩)

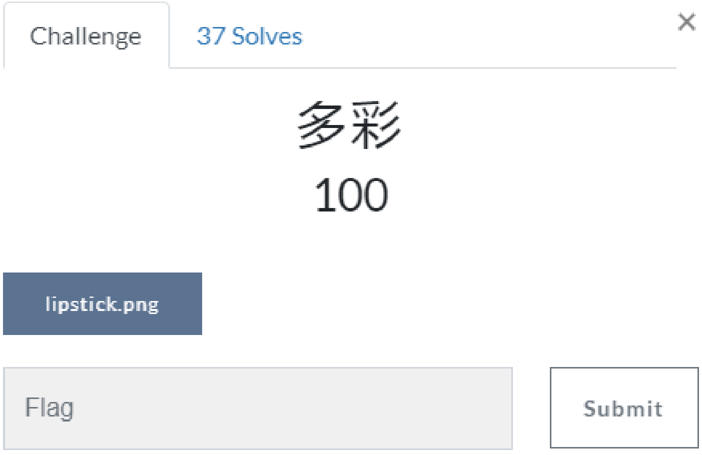
原创

....彬 于 2018-09-21 18:49:55 发布 25362 收藏 1
分类专栏： ctf 文章标签： ctf bugku lipstick bugku多彩

本文链接：https://blog.csdn.net/x947955250/article/details/82805575
版权

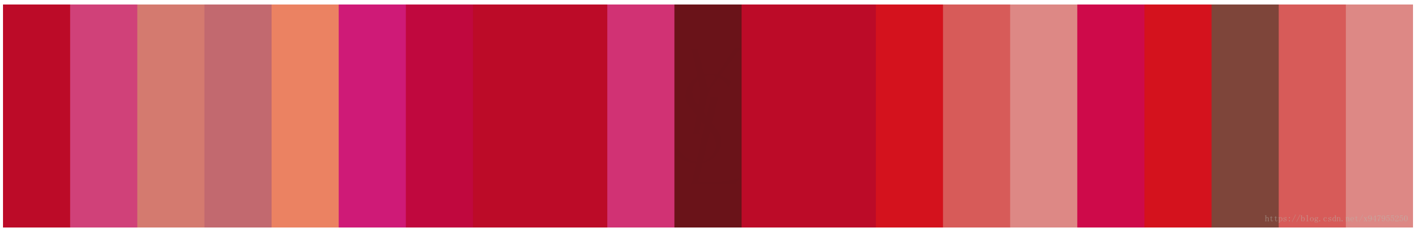

ctf专栏收录该内容
6 篇文章 0 订阅
订阅专栏

一开始是在bugku网站上看到这题的。。后来了解到是N1CTF2018国际赛的题。。

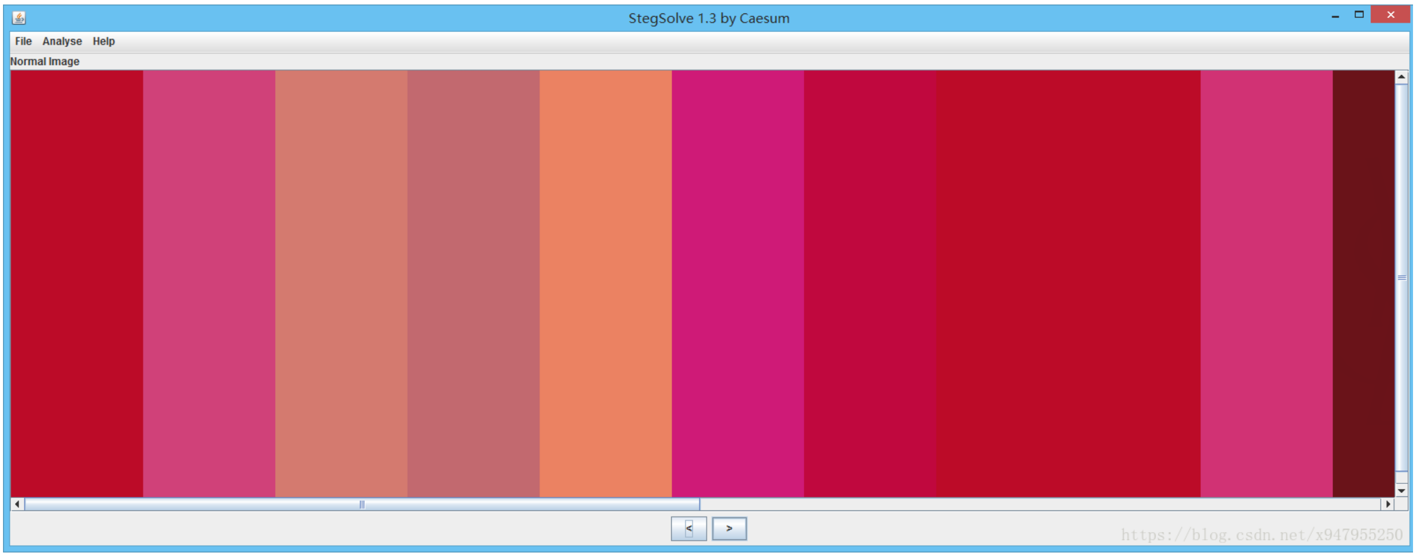


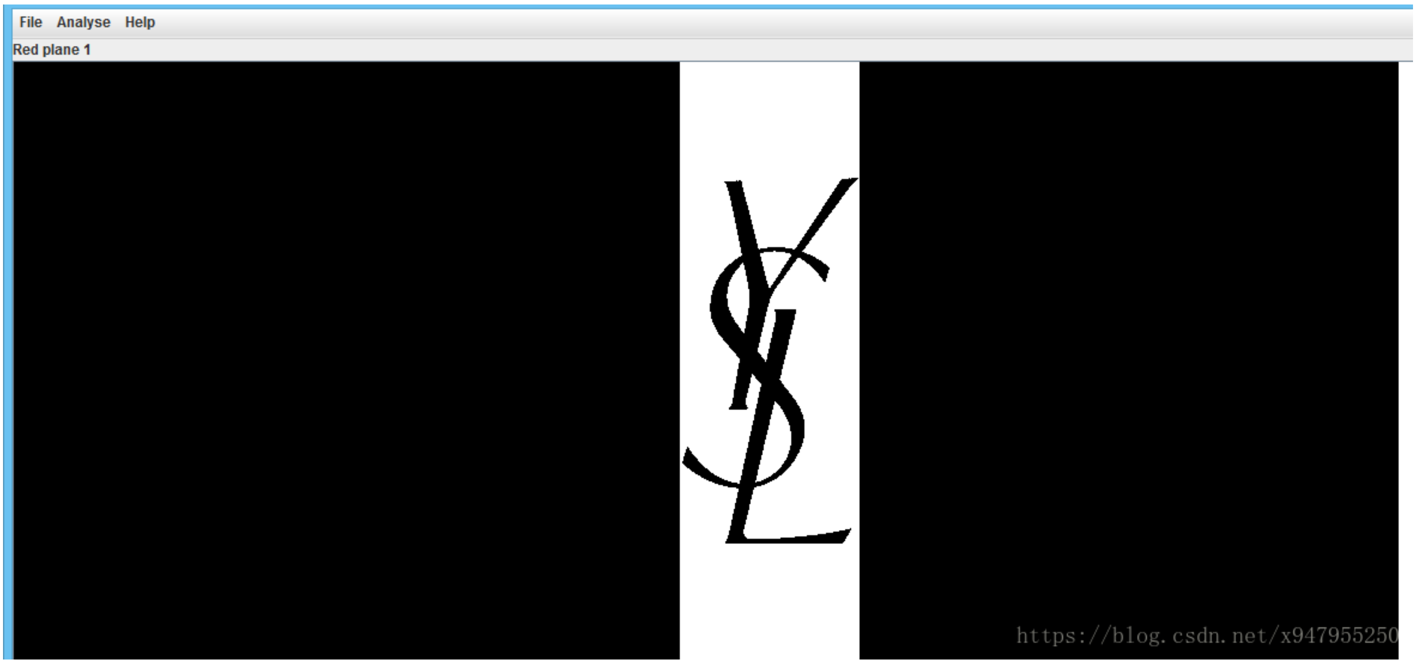
多彩

100



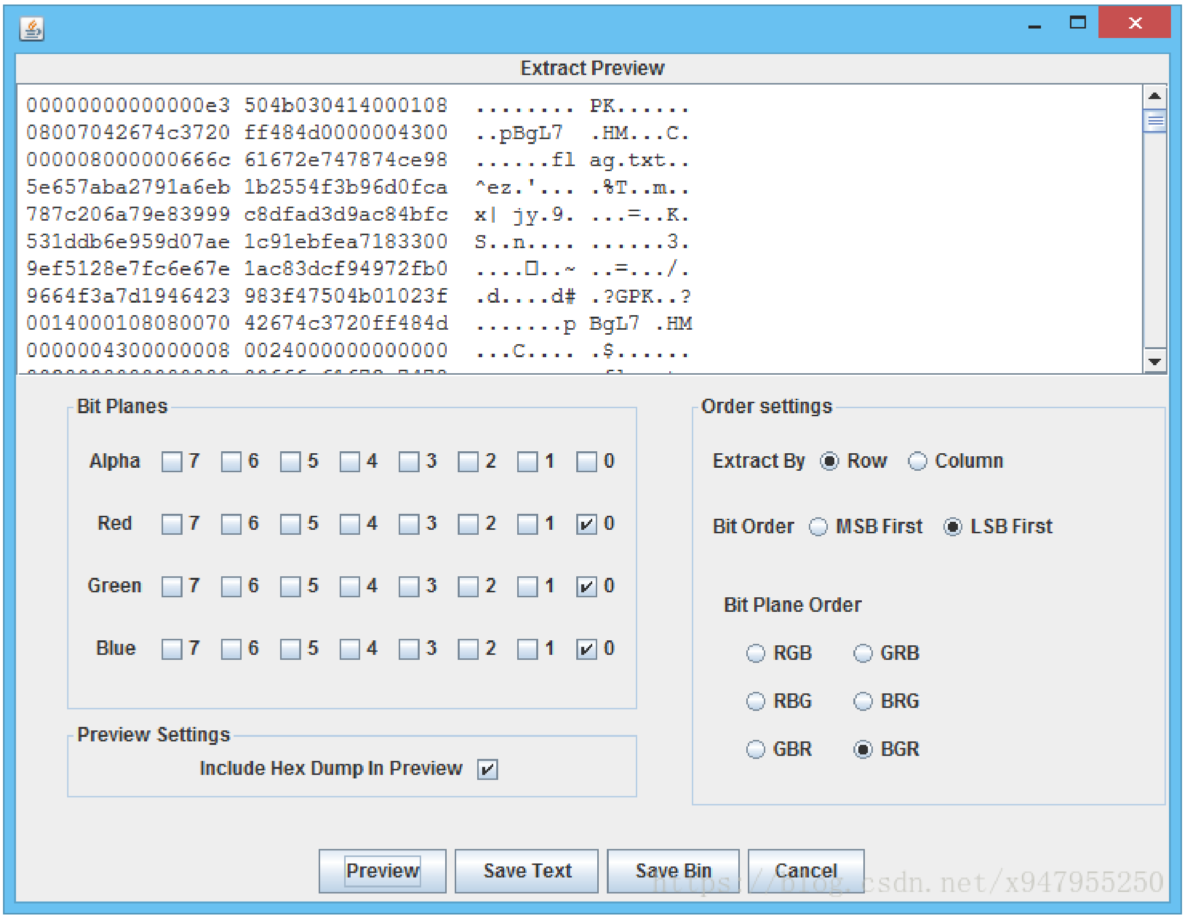
将图片下载下来之后放入Stegsolve。。。





看到了这个。。。(杨树林？？？)再加上题目是lipstick。。。心想着肯定与YSL的口红有关。。。

先分析下。。点击Analyse——>Data Extract



Extract Preview

```
00000000000000e3 504b030414000108  ........ PK......
08007042674c3720 ff484d0000004300  ..pBgL7  .HM...C.
000008000000666c 61672e747874ce98  ......fl ag.txt..
5e657aba2791a6eb 1b2554f3b96d0fca  ^ez.'... .%T..m..
787c206a79e83999 c8dfad3d9ac84bfc  x| jy.9. ...=..K.
531ddb6e959d07ae 1c91ebfea7183300  S..n.... ......3.
9ef5128e7fc6e67e 1ac83dcf94972fb0  ....□..~ ..=.../.
9664f3a7d1946423 983f47504b01023f  .d....d# .?GPK..?
0014000108080070 42674c3720ff484d  .......p BgL7 .HM
0000004300000008 0024000000000000  ...C.... .$......
```

Bit Planes

Alpha	□ 7	□ 6	□ 5	□ 4	□ 3	□ 2	□ 1	□ 0
Red	□ 7	□ 6	□ 5	□ 4	□ 3	□ 2	□ 1	☑ 0
Green	□ 7	□ 6	□ 5	□ 4	□ 3	□ 2	□ 1	☑ 0
Blue	□ 7	□ 6	□ 5	□ 4	□ 3	□ 2	□ 1	☑ 0

Preview Settings

Include Hex Dump In Preview ☑

Order settings

Extract By ● Row ○ Column

Bit Order ○ MSB First ● LSB First

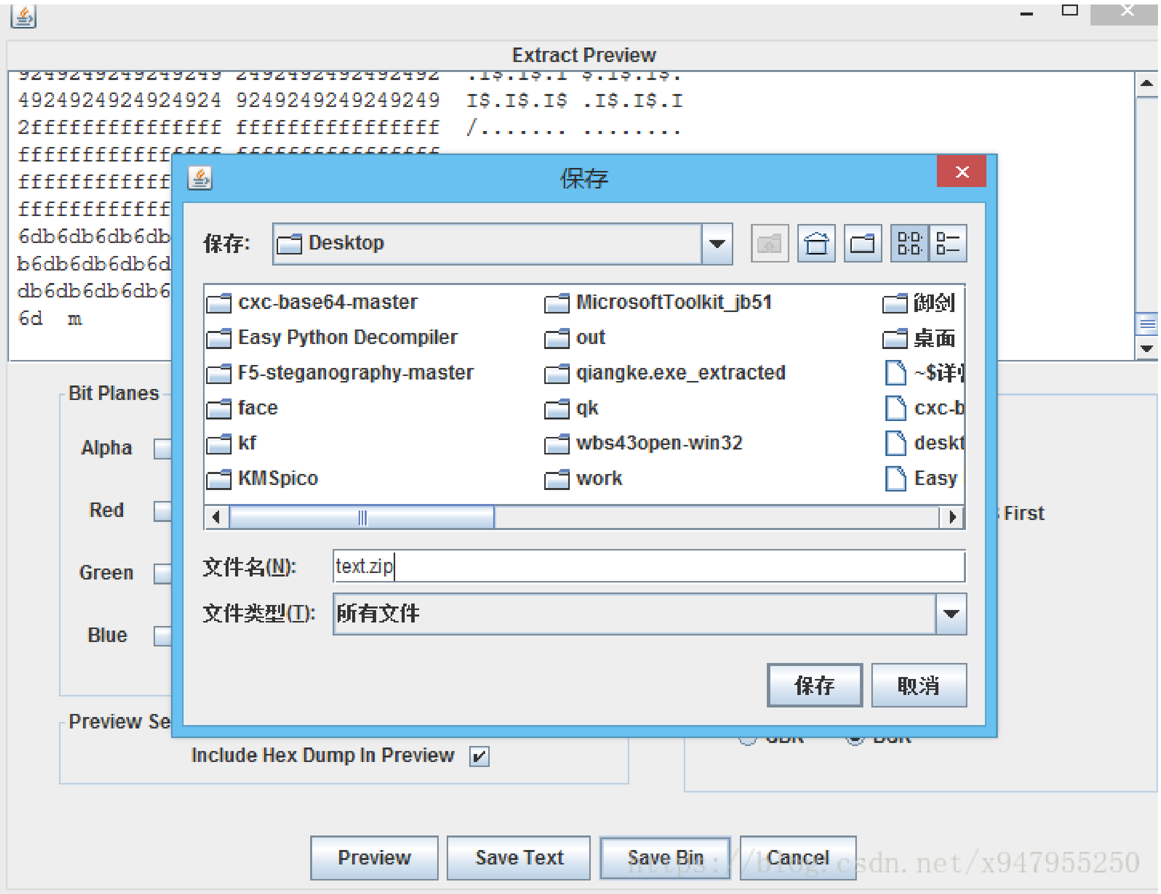
Bit Plane Order

○ RGB ○ GRB

○ RBG ○ BRG

○ GBR ● BGR

看到有个PK头。。心里有数。。直接save bin 存为zip格式



Extract Preview

```
9249249249249249 2492492492492492  .I$.I$.I $.I$.I$.
4924924924924924 9249249249249249  I$.I$.I$ .I$.I$.I
2fffffffffffffff ffffffffffffffff  /....... ........
ffffffffffffffff ffffffffffffffff
ffffffffffff
ffffffffffff
6db6db6db6db
b6db6db6db6d
db6db6db6db6
6d   m
```

保存

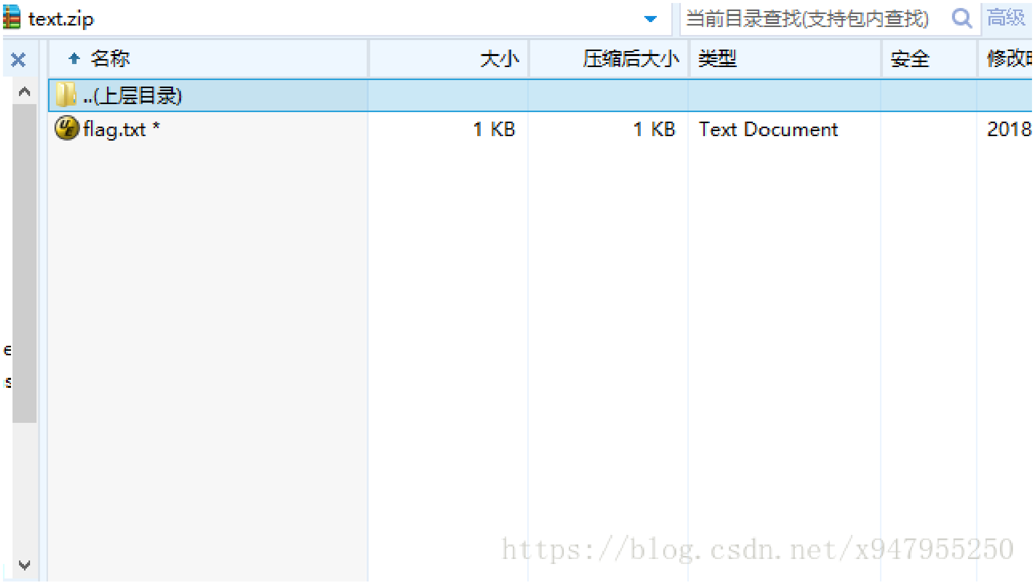
保存: Desktop

文件名(N): text.zip

文件类型(T): 所有文件

Include Hex Dump In Preview ☑

打开压缩包。。发现是加密的。。

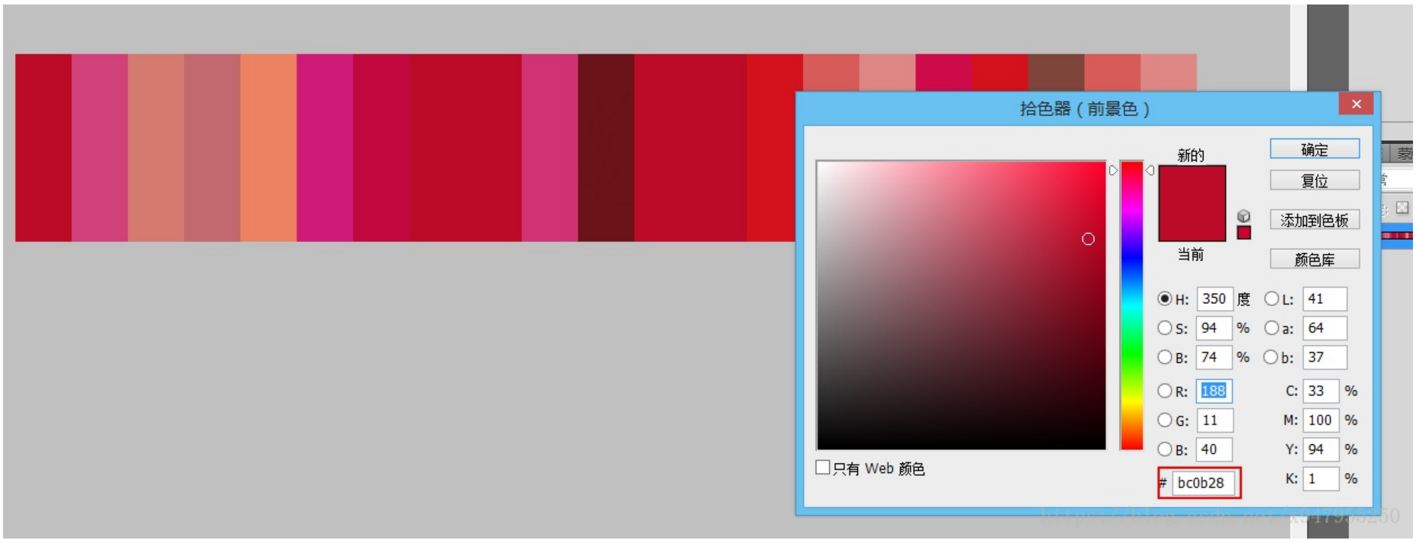


名称	大小	压缩后大小	类型	安全	修改日
..(上层目录)					
flag.txt *	1 KB	1 KB	Text Document		2018

经过尝试发现并不是zip伪加密。。。后来实在猜不到密码。。就上网找了下wp。。发现密码竟然是YSL对应口红色号的二进制转字符串。。。(心态有点崩)。。。这里附上wp的地址

https://www.secpulse.com/archives/69465.html

行吧。。先打开PS取色。。



● H: 350 度　○ L: 41
○ S: 94 %　○ a: 64
○ B: 74 %　○ b: 37
○ R: 188　C: 33 %
○ G: 11　M: 100 %
○ B: 40　Y: 94 %
# bc0b28　K: 1 %

记下这21个颜色代码。。。

然后就去找YSL的口红色号(手动捂脸。。)

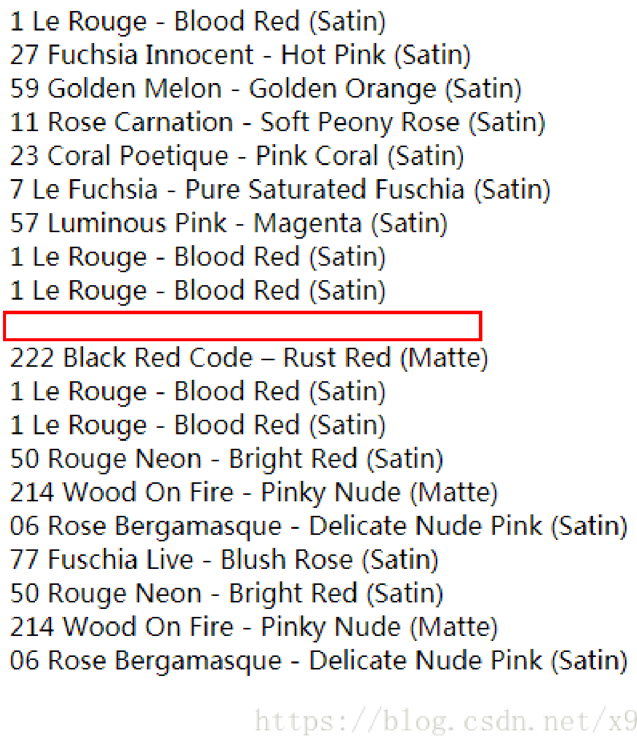
https://www.yslbeautyus.com/on/demandware.store/Sites-ysl-us-Site/en_US/Product-Variation?pid=194YSL

这里我用php写了个脚本。。(为什么不用python。。因为python没学好。。)

```
<?php
        $data='';
        $ch = curl_init();
            curl_setopt($ch, CURLOPT_URL,'https://www.yslbeautyus.com/on/demandware.store/Sites-ysl-us-Site
            curl_setopt($ch, CURLOPT_POST, 1);
            curl_setopt($ch, CURLOPT_POSTFIELDS, $data);
            //curl_setopt($ch, CURLOPT_HTTPHEADER,$data);
            curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
            curl_setopt($ch, CURLOPT_HEADER, 0);
            curl_setopt($ch, CURLOPT_USERAGENT, 'Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.1.5
            curl_setopt($ch, CURLOPT_FOLLOWLOCATION,1);
            $rr=curl_exec($ch);
            curl_close($ch);
            $pat='/style="background-color: #(.*?)" title="(.*?)">/';
            preg_match_all($pat,$rr,$dd);
            $color=array_flip($dd[1]);
            $num=$dd[2];
            //print_r($num);die;
            $arr=array('BC0B28','D04179','D47A6F','C2696F','EB8262', 'CF1A77','C0083E','BC0B28','BC0B28','D
            foreach ($arr as $k => $v) {
                  if(in_array($v,$color))
                  {
                        print_r($num[$color[$v]]);
                        echo "<br />";
                  }

            }
```

运行之后发现。。。



```
1 Le Rouge - Blood Red (Satin)
27 Fuchsia Innocent - Hot Pink (Satin)
59 Golden Melon - Golden Orange (Satin)
11 Rose Carnation - Soft Peony Rose (Satin)
23 Coral Poetique - Pink Coral (Satin)
7 Le Fuchsia - Pure Saturated Fuschia (Satin)
57 Luminous Pink - Magenta (Satin)
1 Le Rouge - Blood Red (Satin)
1 Le Rouge - Blood Red (Satin)

222 Black Red Code – Rust Red (Matte)
1 Le Rouge - Blood Red (Satin)
1 Le Rouge - Blood Red (Satin)
50 Rouge Neon - Bright Red (Satin)
214 Wood On Fire - Pinky Nude (Matte)
06 Rose Bergamasque - Delicate Nude Pink (Satin)
77 Fuschia Live - Blush Rose (Satin)
50 Rouge Neon - Bright Red (Satin)
214 Wood On Fire - Pinky Nude (Matte)
06 Rose Bergamasque - Delicate Nude Pink (Satin)
```

少了一个色号。。。（心态又崩了。。可能是因为网站更新了。。找不到这个色号。。）

后来翻了一些其他的网站发现空着的色号是76(当然。。看一下别人的wp也能发现)

现在就可以将这些色号编码转为二进制。。然后再转为字符串。。

这里就需要用python了。。(因为这个转换不难。。刚好会)

```
# -*- coding:utf8 -*-
import sys
import libnum

ss=''
s=[1,27,59,11,23,7,57,1,1,76,222,1,1,50,214,6,77,50,53,214,6]
for i in s:
 ss+=bin(i)[2:]
print ss
type = sys.getfilesystemencoding()

print libnum.b2s(ss).decode('utf-8').encode(type)
```

这里需要安装libnum库。。。

github地址

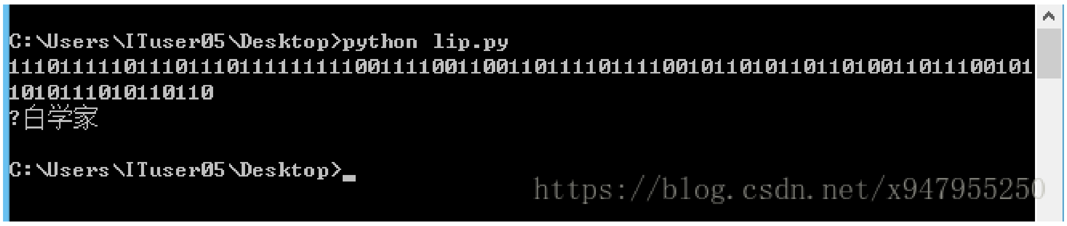
https://github.com/hellman/libnum

直接就python setup.py install

详情可以参考这篇博客

https://www.cnblogs.com/pcat/p/7225782.html

运行脚本得出密码

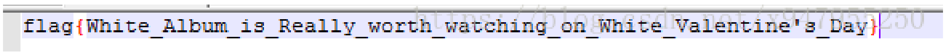


```
C:\Users\ITuser05\Desktop>python lip.py
11101111101110111011111111100111100110011011110111100101101011011010011011100101
1010111010110110
?白学家

C:\Users\ITuser05\Desktop>_
```

密码为白学家。。。。(竟然还是中文的。。心态又崩了)

flag



```
flag{White_Album_is_Really_worth_watching_on_White_Valentine's_Day}
```