[BUGKU] [MISC] 多彩

原创

三无提督w 于 2020-07-10 00:01:33 发布 314 收藏

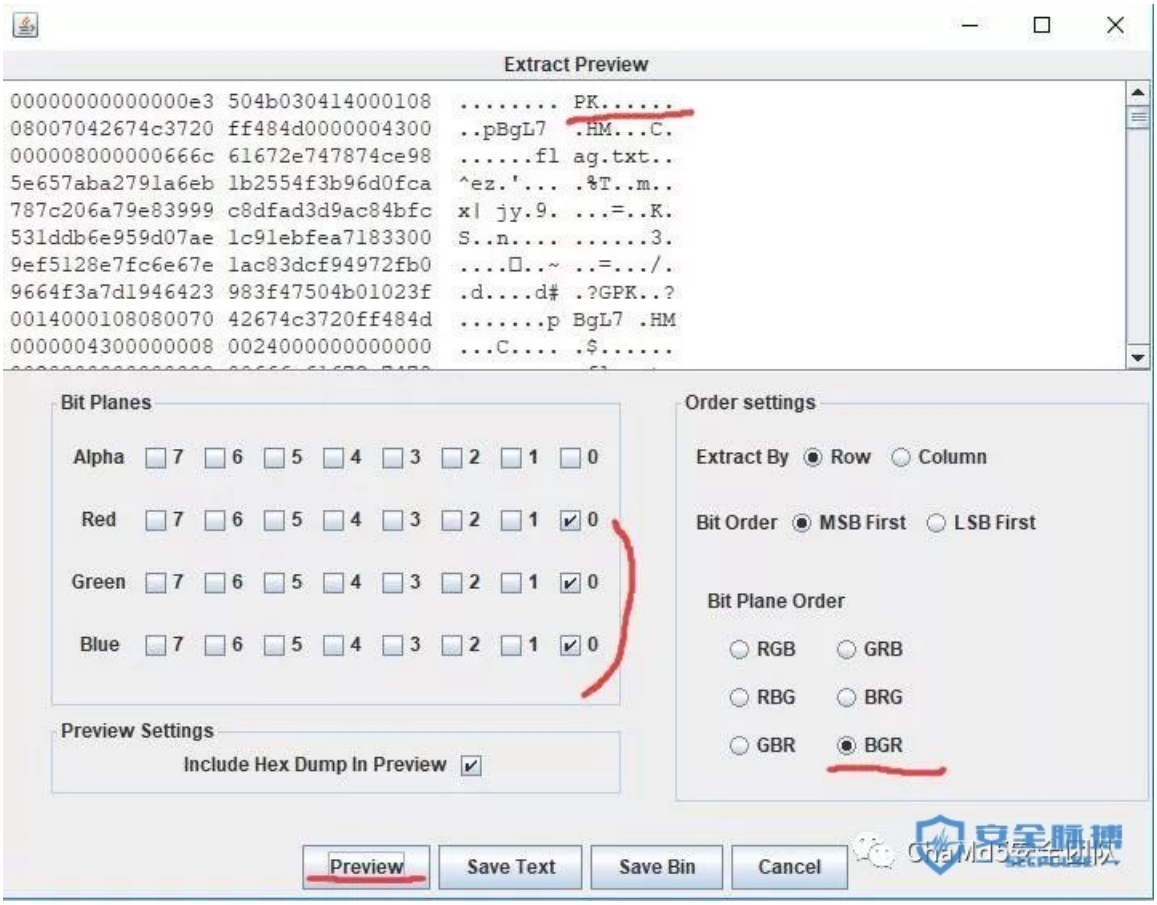
本文链接：https://blog.csdn.net/cf260469080/article/details/107240632

bugku从n1ctf 2018偷的题目，比赛的杂项都是偏门的离谱

当初没做出来，看了writeup后感觉很难受，太偏了，直接贴我看的wp，也是业内老师傅ChaMD5写的wp，我仅仅优化了排版

首先使用隐写神器`Stegsolve`

在中间地带发现了YSL（杨树林，b（￣▽￣）d）这个口红品牌的字样。再继续深入，Analyse→Data Extract



Save Bin保存为一个zip包

这里用winrar打开会报错，得用7z等压缩工具打开才可以。

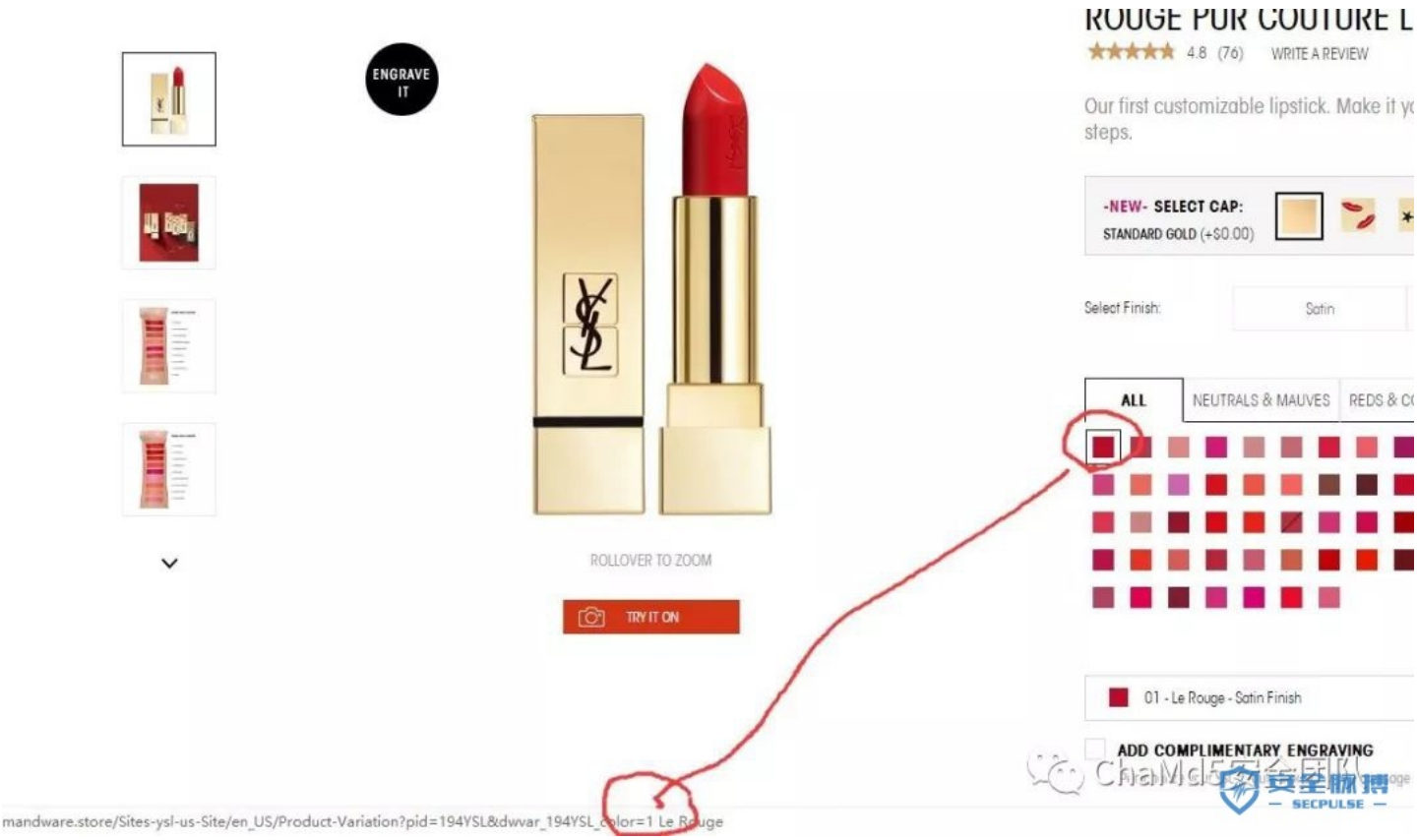
尝试了下伪加密，无果。于是整个过程就剩下一个密码。一般来说图片隐写的话，要么是二进制里藏了东西，要么就是图形藏了东西。这里二进制里藏了zip包，剩下的密码就只能从图形里入手。图形里是21个颜色格，我分别取色

```
BC0B28D04179D47A6FC2696FEB8262CF1A77C0083EBC0B28BC0B28D132746A1319BC0B28BC0B28D4121DD75B59DD8885CE0A4AD4121D7E453AD75B59DD8885
```

这里折腾了好久，发现是要找颜色所对应的YSL口红的色号(lll￣ω￣)

搜到一个网址：

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



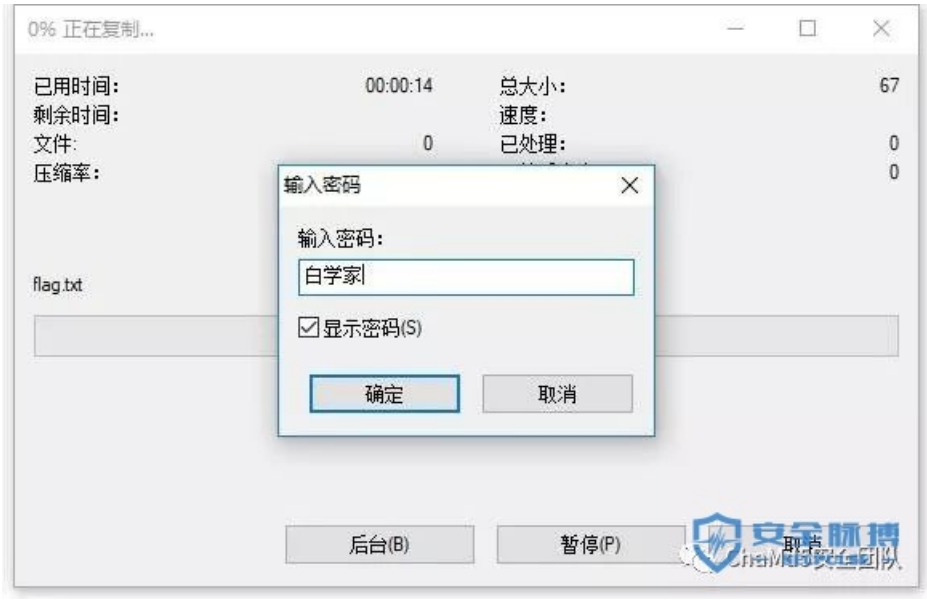
这里颜色值可以对应上色号，于是写脚本收集颜色值对应的色号，并把色号转换为二进制，再组合，再bin2text

```
# -*- coding:utf8 -*-
__author__='pcat@chamd5.org'
import requestsimport re
import libnum

def foo():
url=r'https://www.yslbeautyus.com/on/demandware.store/Sites-ysl-us-Site/en_US/Product-Variation?pid=194YSL'
cont=requests.get(url).content
# print cont
pattern=r'YSL_color=(.*?)%20[sS]*?background-color: #(.*?)"'
rst=re.findall(pattern,cont)
dYSL={}
for num,color in rst:
dYSL[color]=int(num.lstrip('0'))
lst=['BC0B28','D04179','D47A6F','C2696F','EB8262', 'CF1A77','C0083E','BC0B28','BC0B28','D13274', '6A1319','BC0B2
8','BC0B28','D4121D','D75B59', 'DD8885','CE0A4A','D4121D','7E453A','D75B59', 'DD8885']
flag=''.join('{:b}'.format(dYSL[i]) for i in lst)
print libnum.b2s(flag)
pass

if __name__ == '__main__':
foo()
print 'ok'
```

打印出来是“白学家”，用7z进行解压缩



解压后打开flag.txt即可。

---

flag{White_Album_is_Really_worth_watching_on_White_Valentine’s_Day}

~~出题人老白学家了，白雪家给爷死！不对我好像也是白学家，那没事了。~~