

蓝盾杯writeup

转载

[weixin_30364147](#) 于 2018-10-29 23:40:00 发布 132 收藏

原文链接: <http://www.cnblogs.com/yang12318/p/9874101.html>

版权

由于比赛时只给了内网，web题目无法复现，这里就简单写一下misc的部分题目

1、眼花了吗

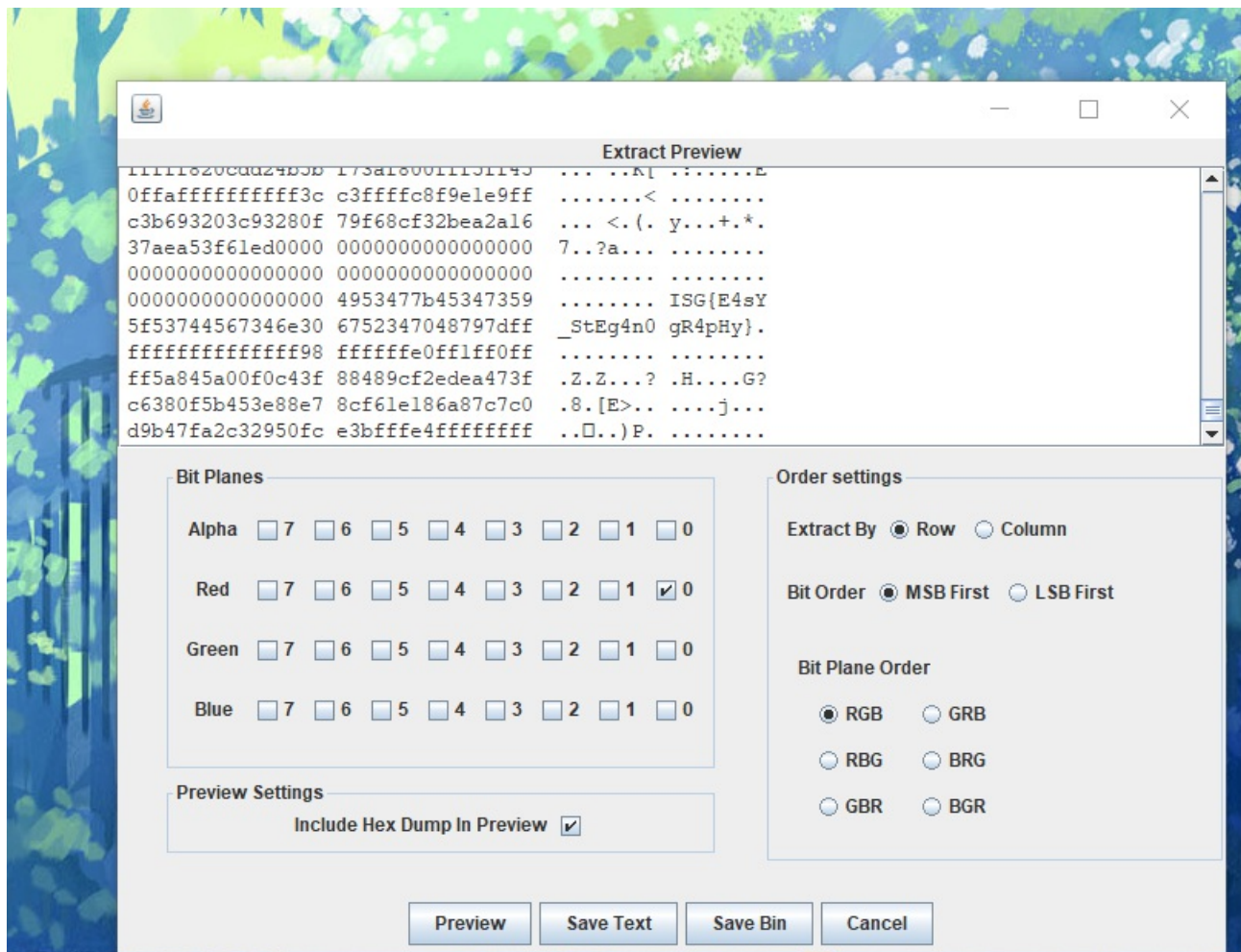
(默默吐槽居然是来自实验吧的原题)

提示：当眼花的时候会显示两张图，可以想到应该是包含双图的情况

用foremost将其分离出来，得到两张相同的图片：



用Stegsolve打开，选择Data Extract，即可以找到flag：



ISG{E4sY_StEg4n0_gR4pHy}

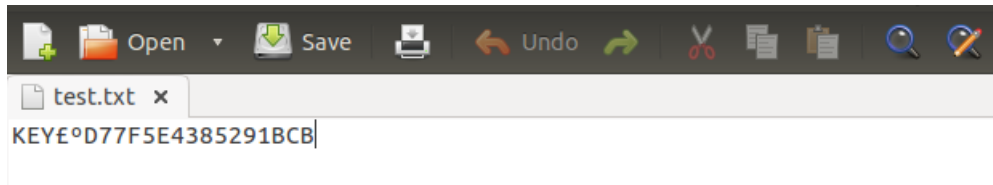
2、好美的玫瑰花

提示：key就在图片里

推测应该是图片里放了key值，用steghide得到key值，但需要知道密码值，首先尝试了弱口令，结果就试出来了

```
guest-RBppyI@ubuntu:~$ steghide extract -sf rose.jpg -p 123456
wrote extracted data to "test.txt".
guest-RBppyI@ubuntu:~$
```

打开test.txt得到key值：



答案即D77F5E4385291BCB

3、BrainFuck

提示：图片很诡异

看到BrainFuck想到使用BrainTools

将下载出来的图片放到bftools.exe在的文件目录下，使用命令：

```
bftools.exe decode braincopter doge.jpg --output --dogeout.jpg
```

再使用：

```
bftools.exe run --dogeout.jpg
```

得到：

```
E:\CTF\BrainTools>bftools.exe decode braincopter doge.jpg --output --dogeout.jpg
E:\CTF\BrainTools>bftools.exe run --dogeout.jpg
Q1RGe0JyYWluZnVjal8xcl9TaWlwMWV9
E:\CTF\BrainTools>
```

即得到一串base64的编码，用converter解码（任何可解base64的工具都可以）得到：

输入(原始值):
Q1RGeQjyYwluZnVja18xc19Taw1wMwV9

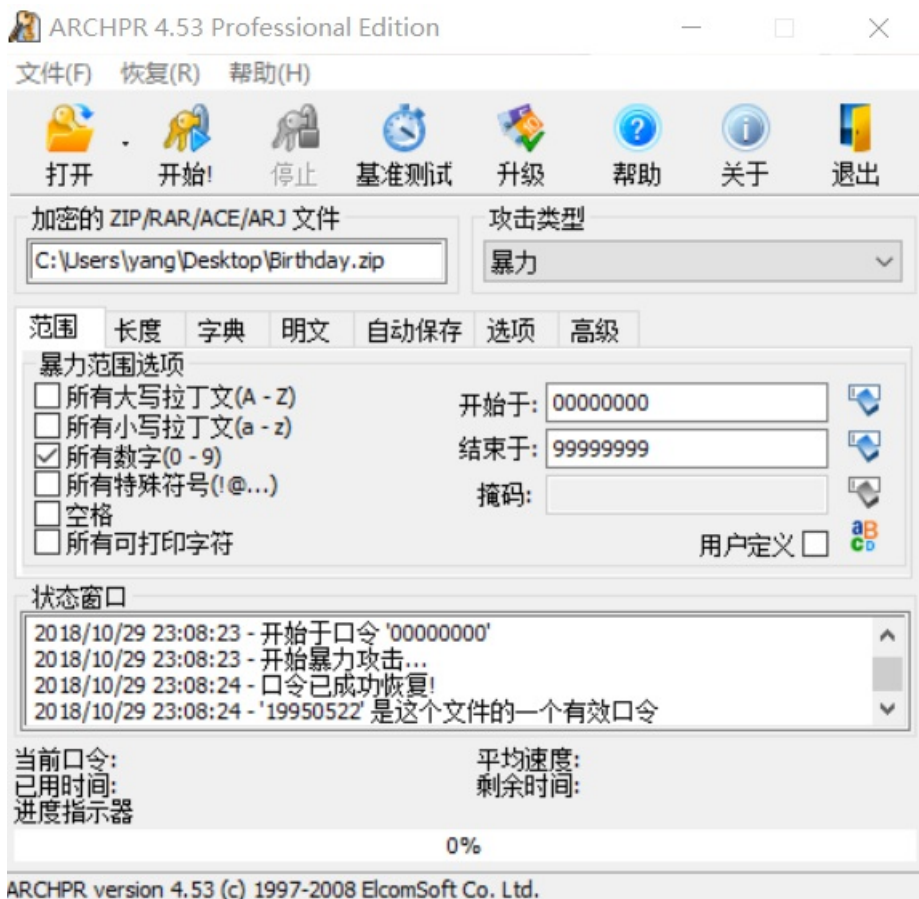
输出(转换值):
CTF{Brainfuck_1s_Simp1e}

即: CTF{Brainfuck_1s_Simp1e}

4、flag就在图片里

打开之后是一个加密的压缩包，因为命名为Birthday.zip，所以考虑密码和生日有关

使用ARCHPR来爆破密码：



得到密码，输入之后得到一张图片，点击查看属性得到flag:



即: BDCTF{gdyh4VOGBD}

转载于:<https://www.cnblogs.com/yang12318/p/9874101.html>