CTF-BUUCTF-MISC

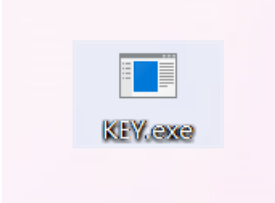
原创

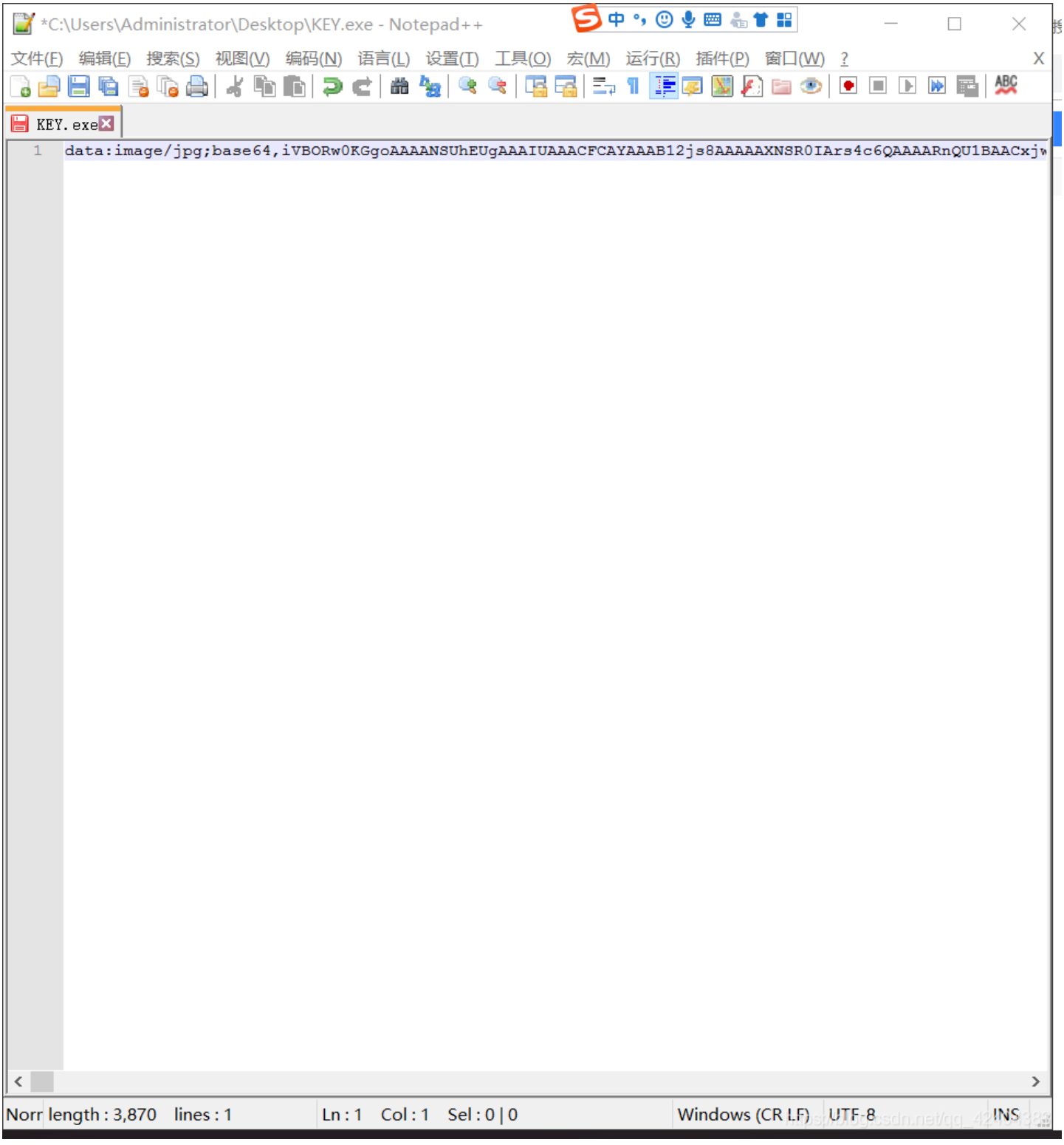
黑仔、 于 2020-01-02 13:42:40 发布 2877 收藏 10

CTF-BUUCTF-MISC

一、N种方法解决

题目：





base64：

标准的Base64并不适合直接放在URL里传输，因为URL编码器会把标准Base64中的“/”和“+”字符变为形如“%XX”的形式，而这些“%”号在存入数据库时还需要再进行转换，因为ANSI SQL中已将“%”号用作通配符。

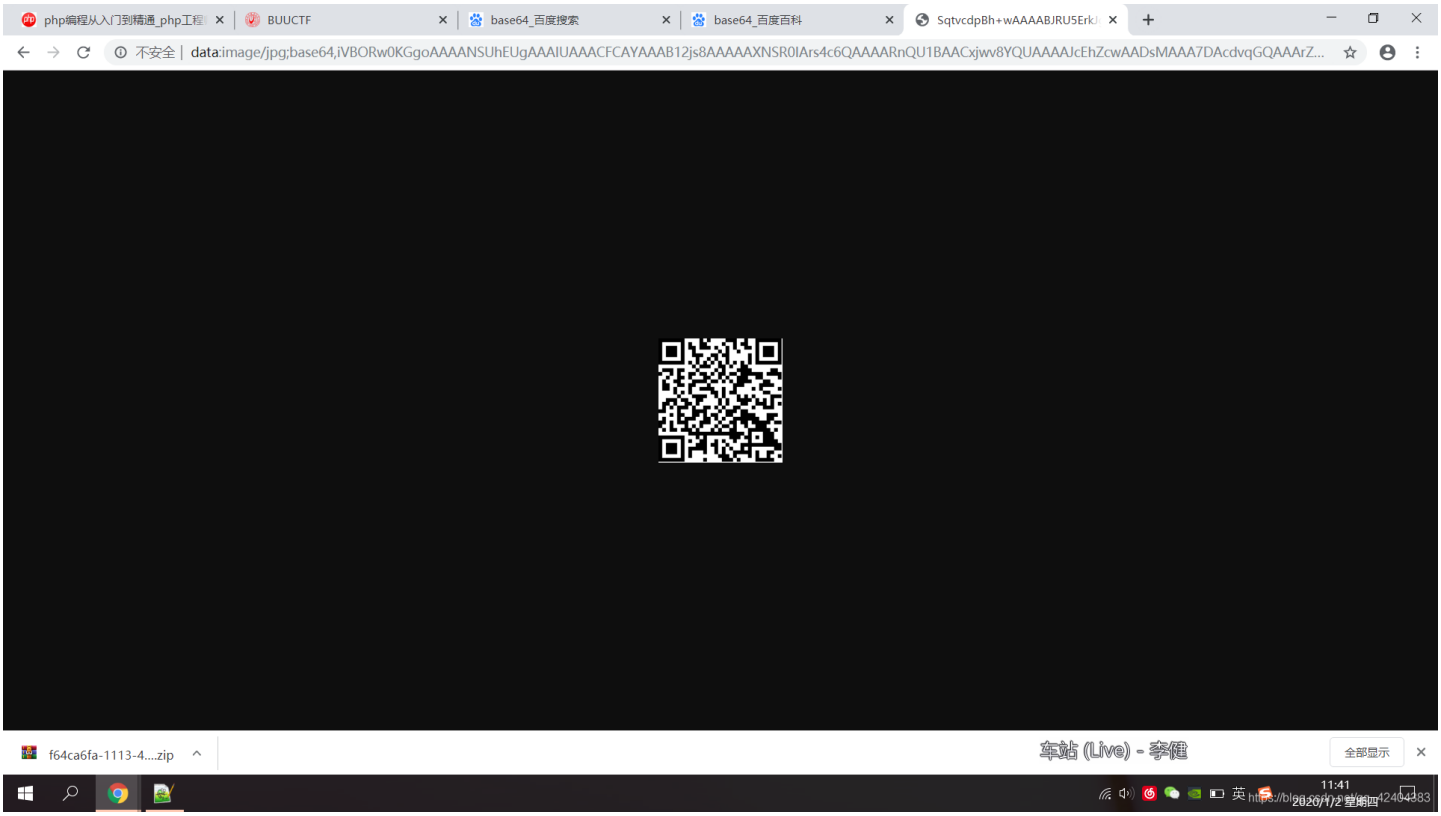
为解决此问题，可采用一种用于URL的改进Base64编码，它在末尾填充'='号，并将标准Base64中的“+”和“/”分别改成了“-”和“_”，这样就免去了在URL编解码和数据库存储时所要作的转换，避免了编码信息长度在此过程中的增加，并统一了数据库、表单等处对象标识符的格式。

另有一种用于正则表达式的改进Base64变种，它将“+”和“/”改成了“!”和“-”，因为“+”,“*”以及前面在IRCu中用到的“[”和“]”在正则表达式中都可能具有特殊含义。

此外还有一些变种，它们将“+/”改为“-”或“.”（用作编程语言中的标识符名称）或“.-”（用于XML中的Nmtoken）甚至“_:”（用于XML中的Name）。

Base64要求把每三个8Bit的字节转换为四个6Bit的字节（3*8* = 4*6* = 24），然后把6Bit再添两位高位0，组成四个8Bit的字节，也就是说，转换后的字符串理论上将要比原来的长1/3。

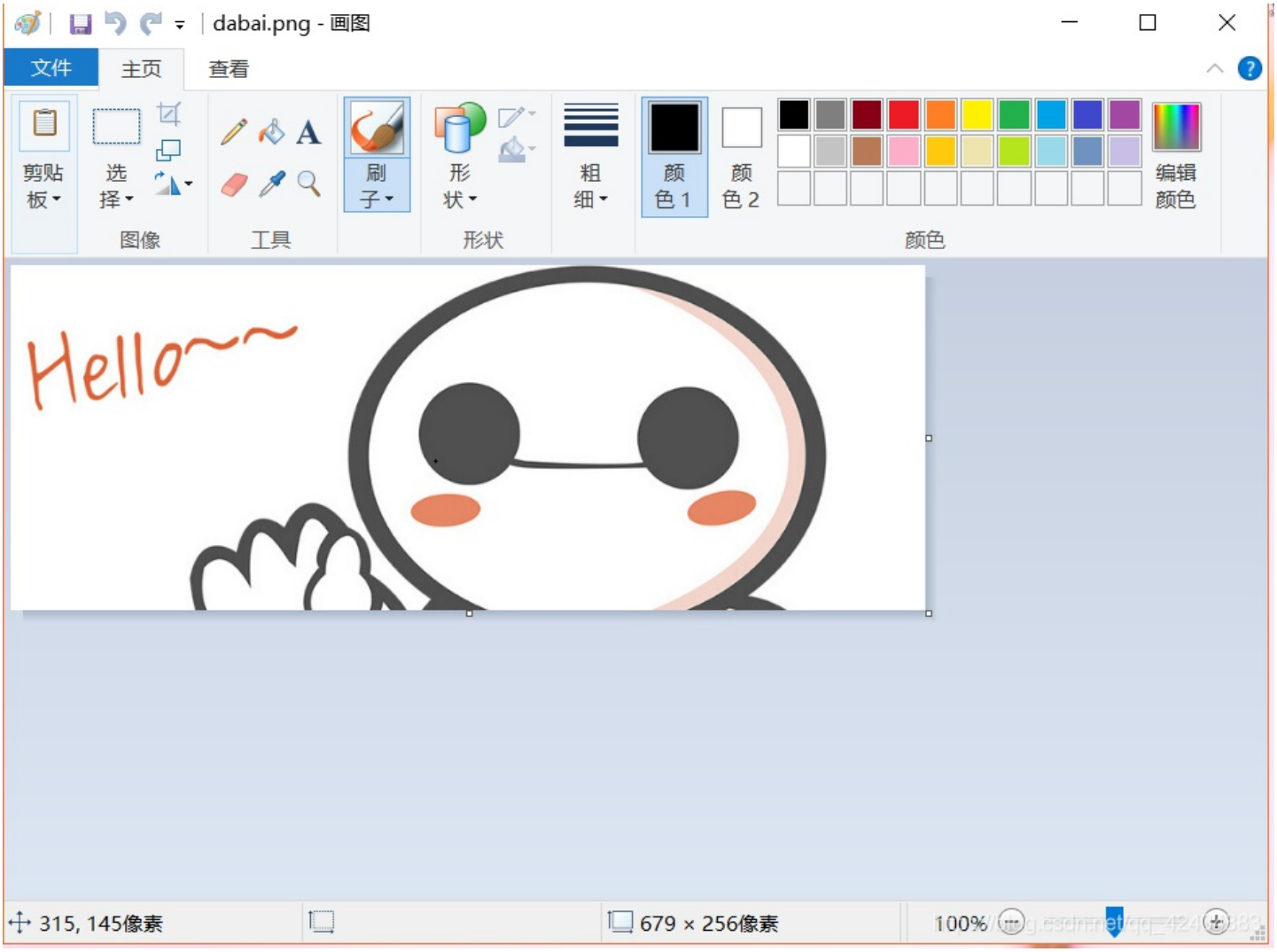
解题：



扫码即可得到flag

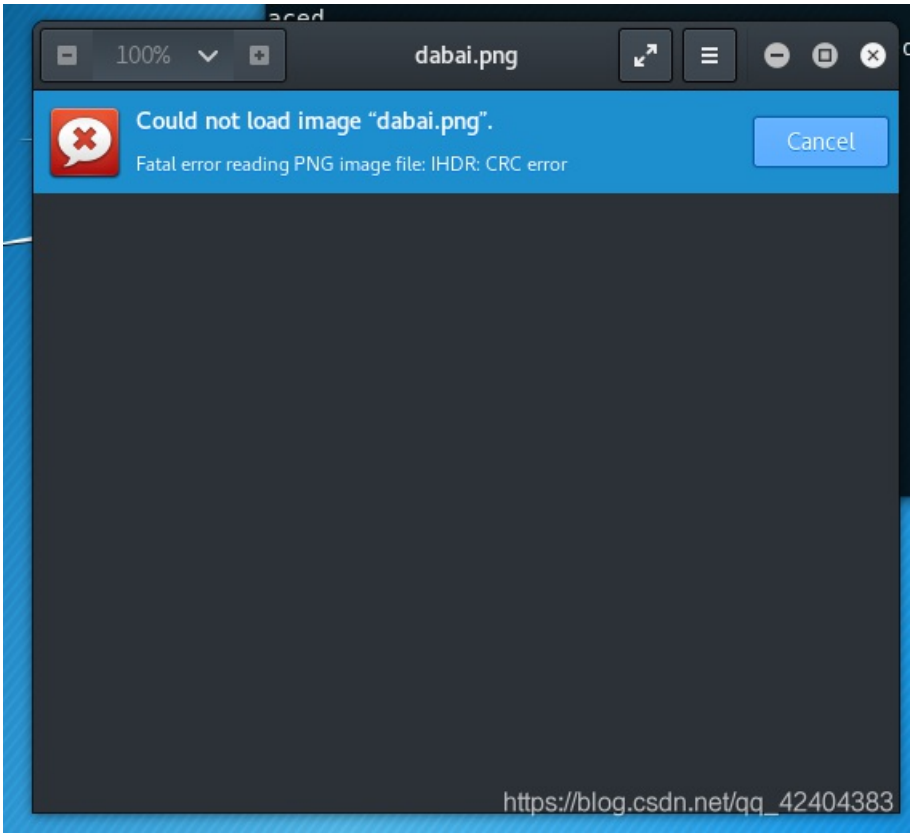
二、大白

看不到图？ 是不是屏幕太小了 注意：得到的 flag 请包上 flag{} 提交




```
root@kali:~# binwalk '/root/Desktop/dabai.png'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 679 x 256, 8-bit/color RGBA, non-interlaced
91            0x5B            Zlib compressed data, compressed

root@kali:~#
```


解题：

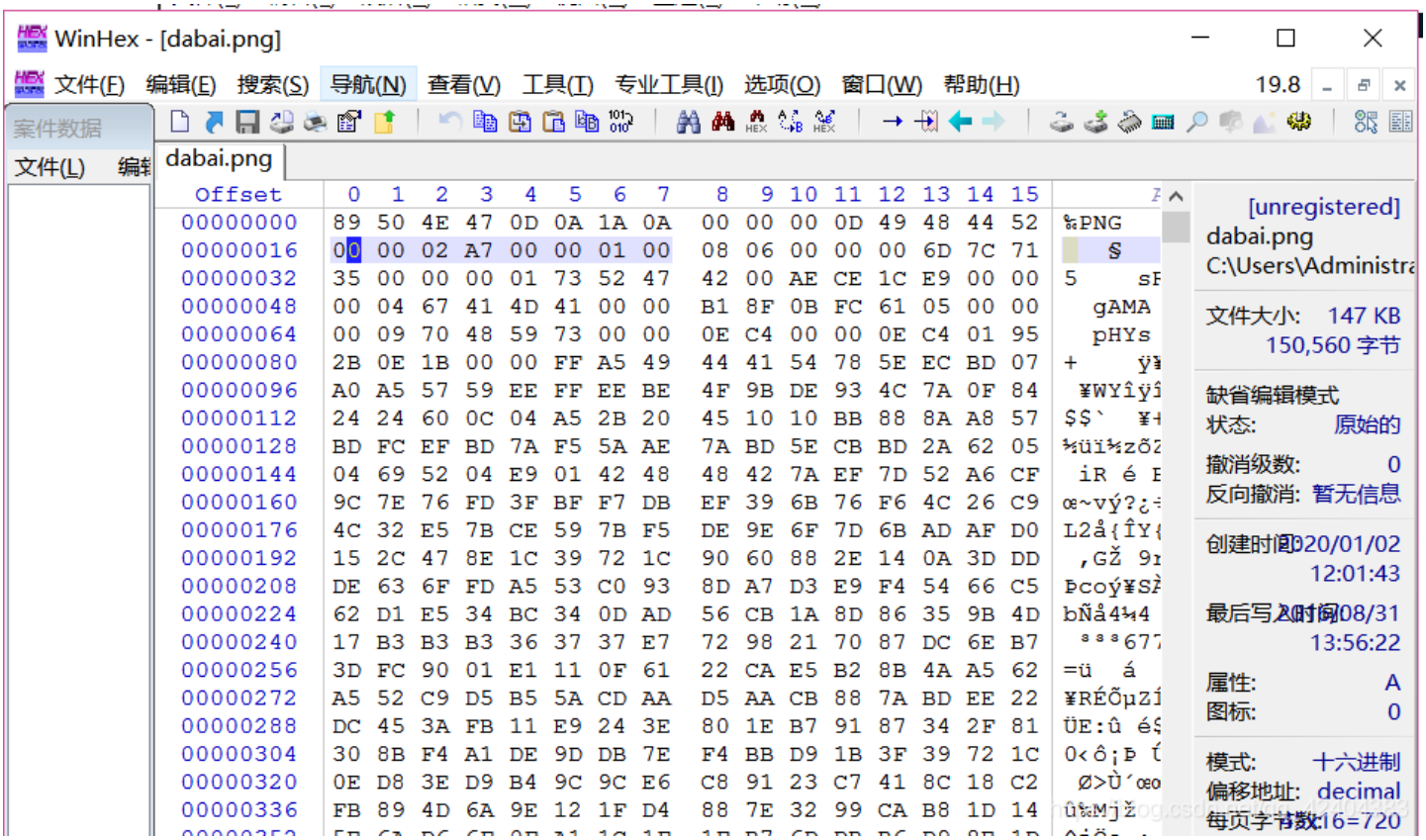


宽和高不匹配打不开、Linux无法打开

根据提示：看不到图？ 是不是屏幕太小了 注意：得到的 flag 请包上 flag{} 提交

改变像素：

用画板改变后无显示、改用winhex



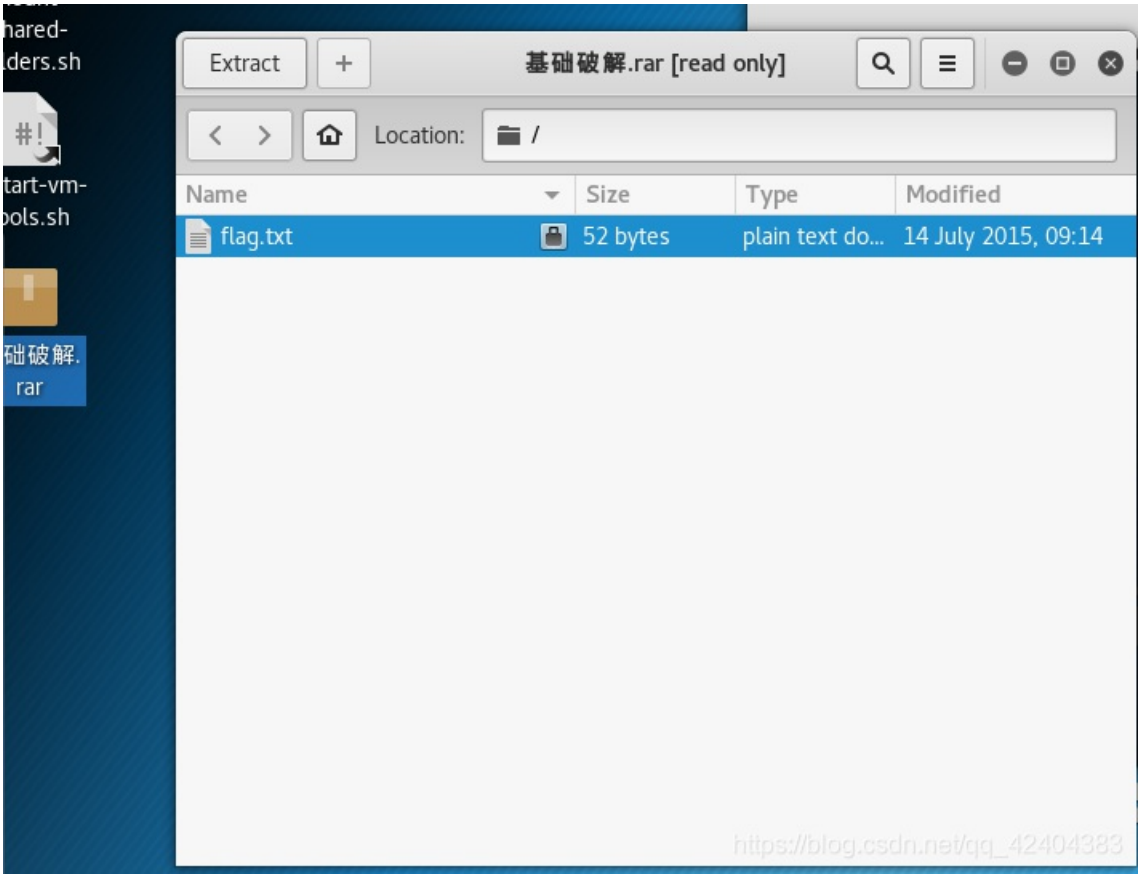
前四位是宽，后四位是高

修改后：00 00 02 00

三、基础破解

给你一个压缩包，你并不能获得什么，因为他是四位数字加密的哈哈哈哈哈哈。。。不对= =我说了什么了不得的东西。。 注意：得到的 flag 请包上 flag{} 提交

题目：



解题：

这里使用的软件名称叫rarcrack，其官方主页: http://rarcrack.sourceforge.net

该软件用于暴力破解压缩文件的密码，但仅支持RAR, ZIP, 7Z这三种类型的压缩包，其特点是可以使用多线程，而且可以随时暂停与继续(暂停时会在当前目录生成一个xml文件，里面显示了正在尝试的一个密码)。

（linux下、kali用apt-get命令）rarcrack安装方法：

首先从官网下载安装包，然后执行如下命令

```
tar -xjf rarcrack-0.2.tar.bz2
cd rarcrack-0.2
make && make install
```

在执行过程中，如果出现如下错误:

```
gcc -pthread rarcrack.cxml2-config --libs --cflags-O2 -o rarcrack
/bin/sh: 1: xml2-config: not found
In file included from rarcrack.c:21:0:
rarcrack.h:25:48: 致命错误： libxml/xmlmemory.h：没有那个文件或目录
编译中断。
make: *** [all] 错误 1
```

那么可以执行`sudo apt-get install libxml2-dev libxslt-dev`进行修复。

rarcrack使用方法：

执行命令: `rarcrack 文件名 -threads 线程数 -type rar|zip|7z`

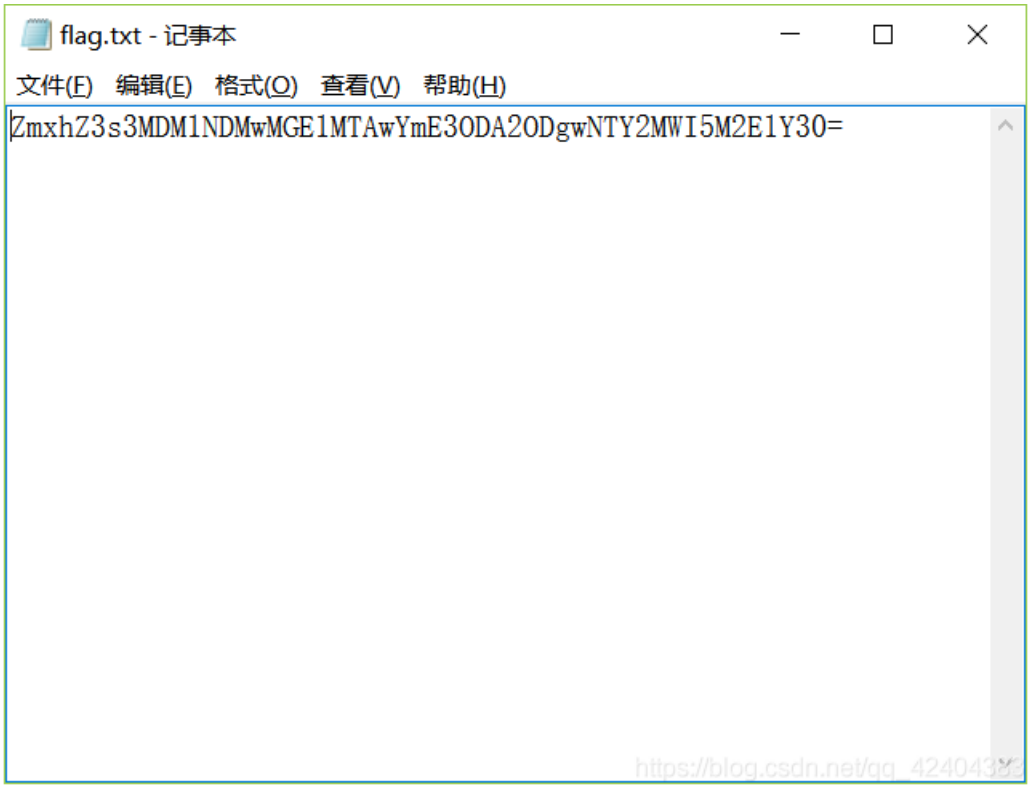
```
[root@iZuf60eeufai4clsvwgn80Z ~]# rarcrack "/root/基础破解.rar" --threads 4 --type rar
RarCrack! 0.2 by David Zoltan Kedves (kedazo@gmail.com)

INFO: the specified archive type: rar
INFO: cracking /root/基础破解.rar, status file: /root/基础破解.rar.xml
INFO: Resuming cracking from password: 'BVe'
Probing: 'CpS' [632 pwds/sec]
Probing: 'CWD' [677 pwds/sec]
Probing: 'DtY' [689 pwds/sec]
Probing: 'E1M' [698 pwds/sec]
```


破解不出来、改变下字典（纯数字、4位）：

```
[root@iZuf60eeufai4clsvwgn80Z ~]# ls
rarcrack-0.2  xampp-linux-x64-7.0.20-0-installer.run  基础破解.rar  基础破解.rar.xml
[root@iZuf60eeufai4clsvwgn80Z ~]# vi 基础破解.rar.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<rarcrack>
  <abc>0123456789</abc>
  <current>0</current>
  <good_password/>
</rarcrack>
~
~
~
~
~
~
~
~
~
~
~
```


得到密码：2563


flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
ZmxhZ3s3MDM1NDMwMGE1MTAwYmE3ODA2ODgwNTY2MWI5M2E1Y30=

解密：

解密：


開く
请将要加密或解密的内容复制到以下区域
flag{70354300a5100ba78068805661b93a5c}
BASE64加密
BASE64解密
广告