




CTF-BUUCTF-MISC

原创

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

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

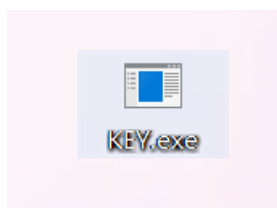
本文链接：https://blog.csdn.net/qq_42404383/article/details/103802903

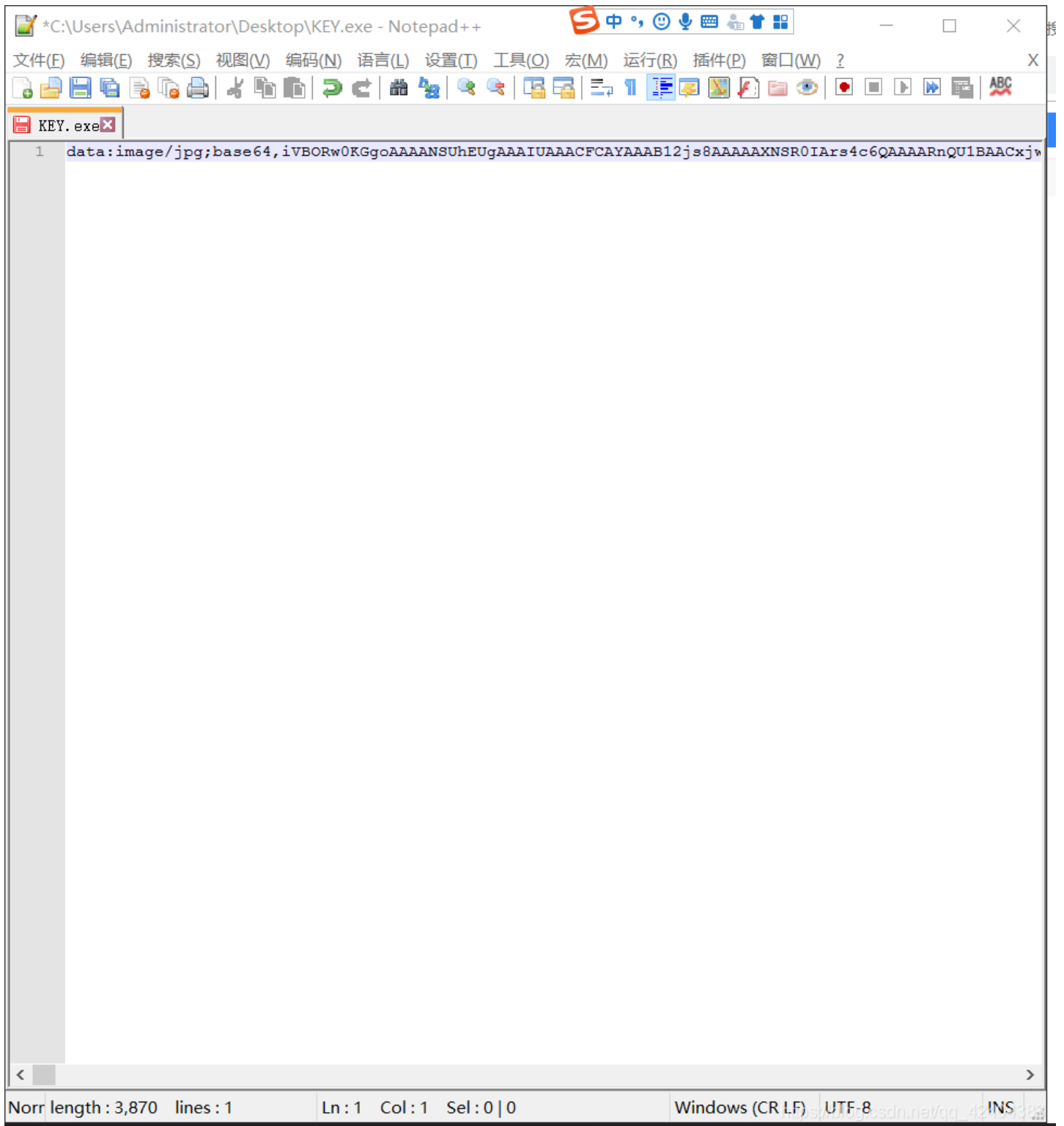
版权

CTF-BUUCTF-MISC

一、N种方法解决

题目：





The image shows a Notepad++ window with the following content:

```
*C:\Users\Administrator\Desktop\KEY.exe - Notepad++
文件(E) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(I) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
KEY.exe x
1 data:image/jpeg;base64,iVBORw0KGgoAAAANSUhEUgAAAIUAAACFCAYAAAB12js8AAAAAXNSR0IArs4c6QAAARnQU1BAACxjw
```

At the bottom of the window, the status bar displays: Norr length : 3,870 lines : 1 Ln : 1 Col : 1 Sel : 0 | 0 Windows (CR LF) UTF-8

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。

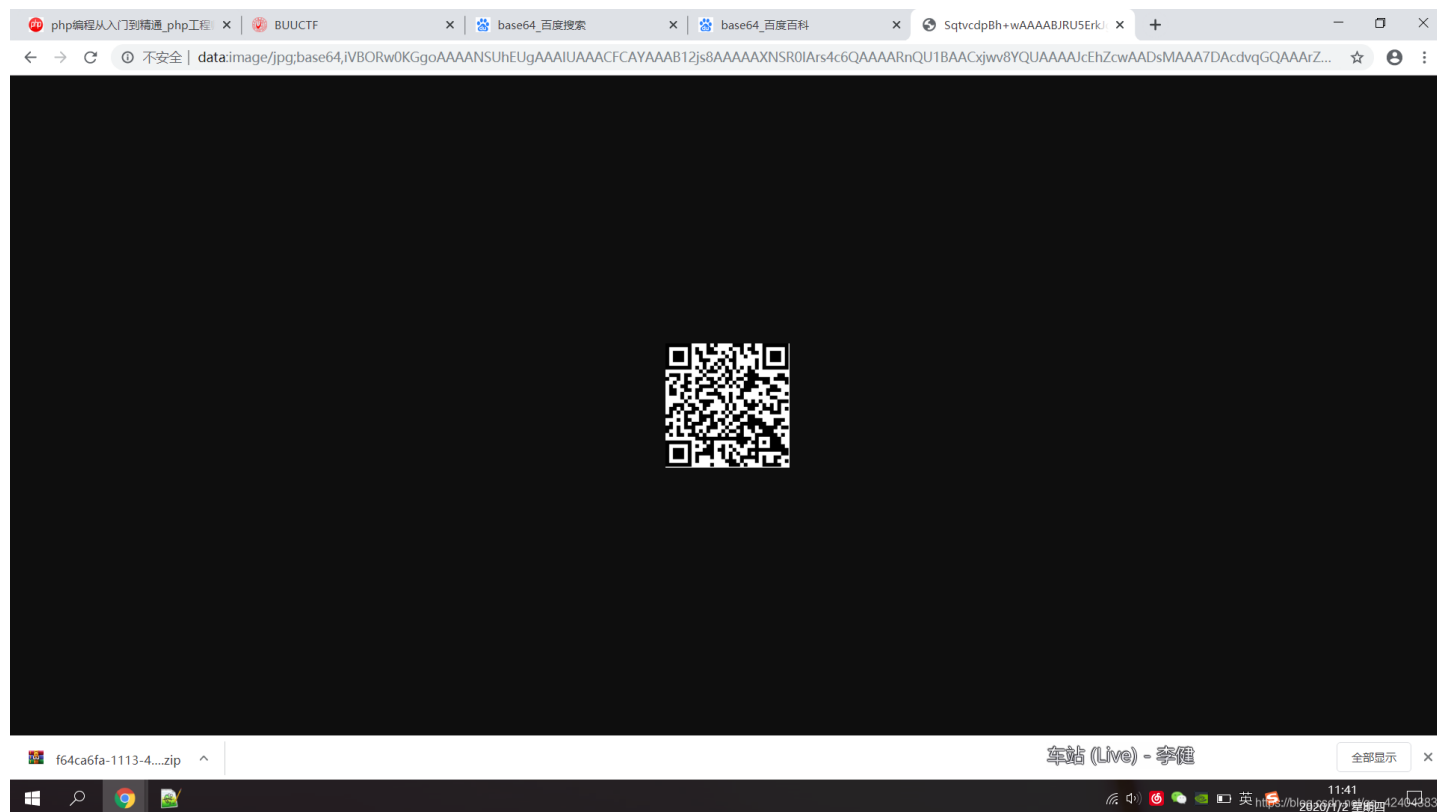
为解决此问题，可采用一种用于URL的改进Base64编码，它在末尾填充‘=’号，并将标准Base64中的“+”和“/”分别改成了“-”和“_”，这样就免去了在URL编解码和数据库存储时所要作的转换，避免了编码信息长度在此过程中的增加，并统一了数据库、表单等处对象标识符的格式。

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（ $3 \times 8 = 4 \times 6 = 24$ ），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。

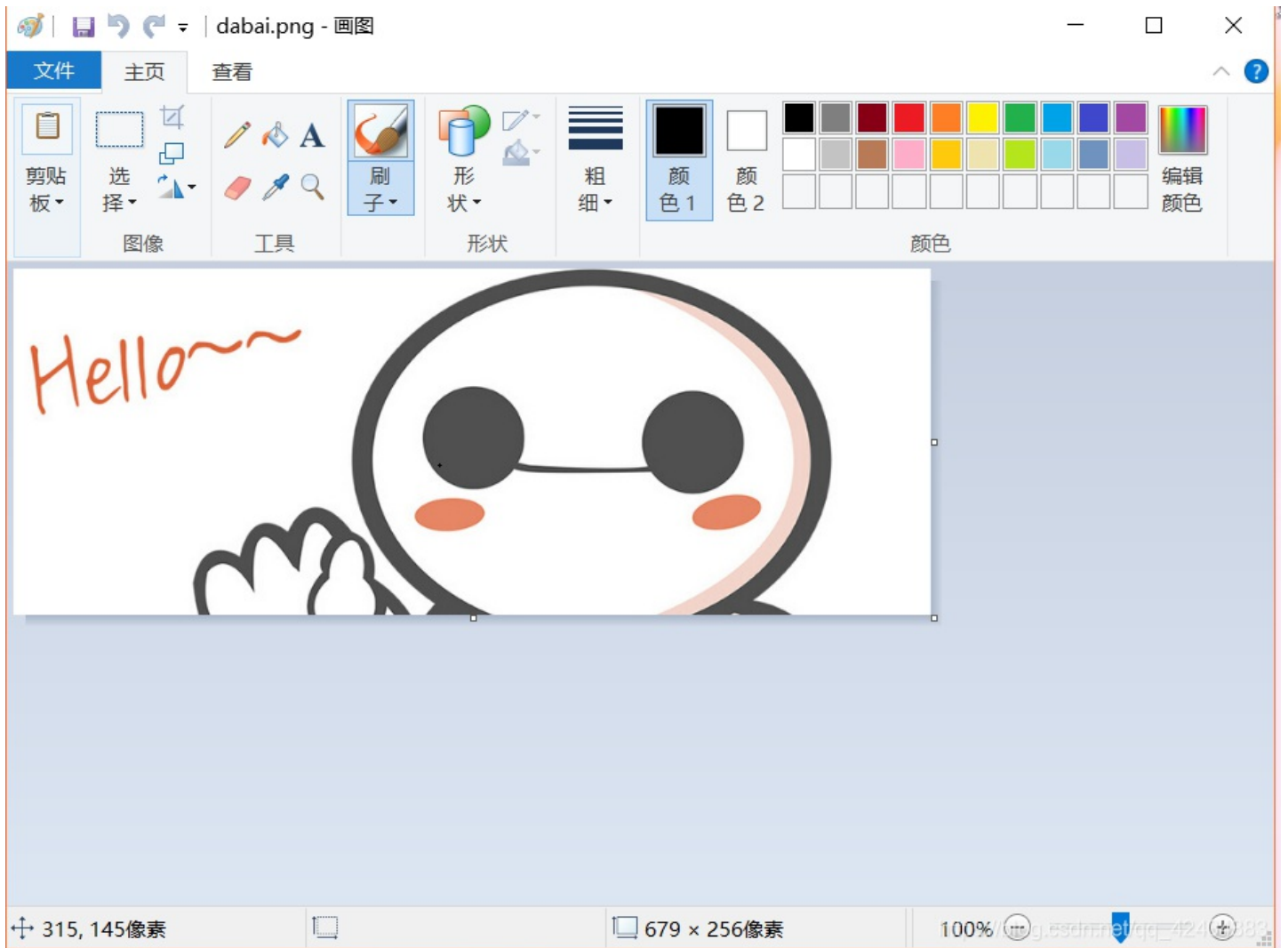
解题：



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'
```

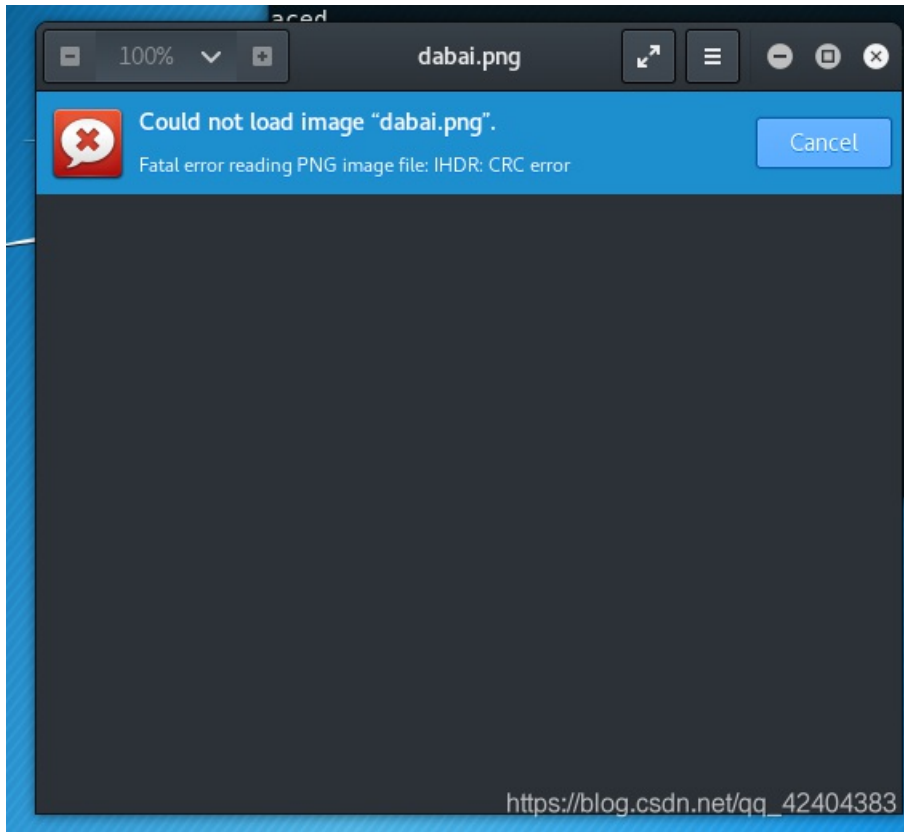
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 679 x 256, 8-bit/color RGBA, non-interlaced
91	0x5B	Zlib compressed data, compressed

```
root@kali:~#
```

restart-vm-tools.sh

https://blog.csdn.net/qq_42404383

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

WinHex - [dabai.png]

文件(E) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H) 19.8

案件数据 dabai.png

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG
00000016	00	00	02	A7	00	00	01	00	08	06	00	00	00	6D	7C	71	\$
00000032	35	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	5 sF
00000048	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	gAMA
00000064	00	09	70	48	59	73	00	00	0E	C4	00	00	0E	C4	01	95	pHYs
00000080	2B	0E	1B	00	00	FF	A5	49	44	41	54	78	5E	EC	BD	07	+ y
00000096	A0	A5	57	59	EE	FF	EE	BE	4F	9B	DE	93	4C	7A	0F	84	WYiYi
00000112	24	24	60	0C	04	A5	2B	20	45	10	10	BB	88	8A	A8	57	\$ \$ ` ¥+
00000128	BD	FC	EF	BD	7A	F5	5A	AE	7A	BD	5E	CB	BD	2A	62	05	üi zöZ
00000144	04	69	52	04	E9	01	42	48	48	42	7A	EF	7D	52	A6	CF	iR é E
00000160	9C	7E	76	FD	3F	BF	F7	DB	EF	39	6B	76	F6	4C	26	C9	œ~vY?¿:
00000176	4C	32	E5	7B	CE	59	7B	F5	DE	9E	6F	7D	6B	AD	AF	D0	L2â{ÎY{
00000192	15	2C	47	8E	1C	39	72	1C	90	60	88	2E	14	0A	3D	DD	,GŽ 9r
00000208	DE	63	6F	FD	A5	53	C0	93	8D	A7	D3	E9	F4	54	66	C5	Ëcoý¥Sž
00000224	62	D1	E5	34	BC	34	0D	AD	56	CB	1A	8D	86	35	9B	4D	bÑâ44
00000240	17	B3	B3	B3	36	37	37	E7	72	98	21	70	87	DC	6E	B7	***677
00000256	3D	FC	90	01	E1	11	0F	61	22	CA	E5	B2	8B	4A	A5	62	=ü á
00000272	A5	52	C9	D5	B5	5A	CD	AA	D5	AA	CB	88	7A	BD	EE	22	¥RÉÖμZí
00000288	DC	45	3A	FB	11	E9	24	3E	80	1E	B7	91	87	34	2F	81	ÛE:û é\$
00000304	30	8B	F4	A1	DE	9D	DB	7E	F4	BB	D9	1B	3F	39	72	1C	0< ô; E í
00000320	0E	D8	3E	D9	B4	9C	9C	E6	C8	91	23	C7	41	8C	18	C2	Ø>Ü´oeso
00000336	FB	89	4D	6A	9E	12	1F	D4	88	7E	32	99	CA	B8	1D	14	û%Mjžog.030
00000352	FB	89	4D	6A	9E	12	1F	D4	88	7E	32	99	CA	B8	1D	14	ûMjžog.030

[unregistered] dabai.png C:\Users\Administrat...
 文件大小: 147 KB
 150,560 字节
 缺省编辑模式
 状态: 原始的
 撤销级数: 0
 反向撤销: 暂无信息
 创建时间: 20/01/02 12:01:43
 最后写入时间: 08/31 13:56:22
 属性: A
 图标: 0
 模式: 十六进制
 偏移地址: decimal
 每页字节数: 16=720

前四位是宽，后四位是高

修改后: 00 00 02 00

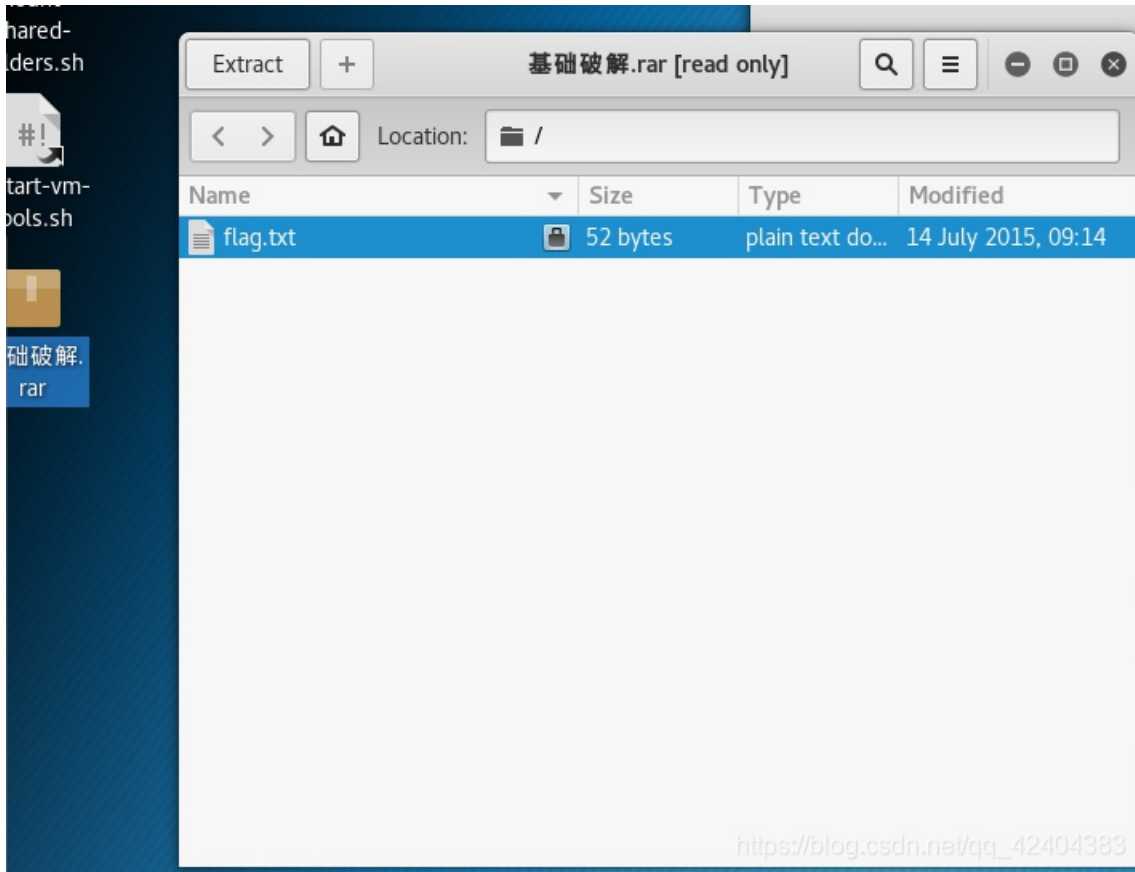


三、基础破解

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。。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]
```

https://blog.csdn.net/qq_42404383

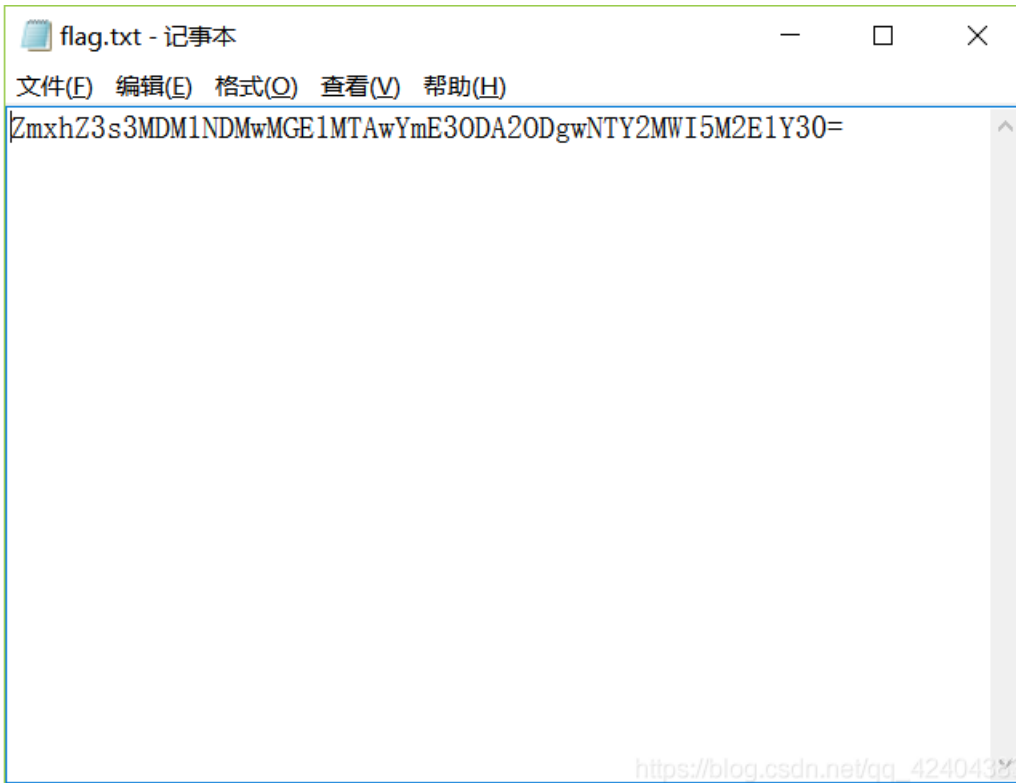
破解不出来、改变下字典（纯数字、4位）：

```
[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>
```

https://blog.csdn.net/qq_42404383

得到密码：2563



解密:

解密:

開<

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

廣告 X

機密桂報，個人桂報保護！

https://blog.csdn.net/qq_42404383