

Bugku—MISC题总结

原创

Sn0w/ 于 2019-06-15 18:59:38 发布 2792 收藏 27

分类专栏: [CTF_Writeup](#) 文章标签: [Bugku MISC](#)

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_43431158/article/details/91400662

版权



[CTF_Writeup](#) 专栏收录该内容

32 篇文章 4 订阅

订阅专栏

前言: MISC考脑洞, 也考分析和观察能力, 总之比较有趣, 就总结一下我的做题过程。

这是一张单纯的图片



https://blog.csdn.net/qq_43431158

用winhex打开

640	1D 64 06 8A 28 03 D0 A8 A2 8A 00 28 A2 8A 00 28	d Š(Đ`ćŠ (ćŠ (
650	A2 8A 00 FF 26 23 31 30 37 3B 26 23 31 30 31 3B	ćŠ ŷke
660	26 23 31 32 31 3B 26 23 31 32 33 3B 26 23 31 32	y{
670	31 3B 26 23 31 31 31 3B 26 23 31 31 37 3B 26 23	1;ou&#
680	33 32 3B 26 23 39 37 3B 26 23 31 31 34 3B 26 23	32;ar&#
690	31 30 31 3B 26 23 33 32 3B 26 23 31 31 34 3B 26	101; r&
6A0	23 31 30 35 3B 26 23 31 30 33 3B 26 23 31 30 34	#105;gh
6B0	3B 26 23 31 31 36 3B 26 23 31 32 35 3B D9 D9	; t}ùù

Unicode编码转换ASCII即可得出flag

隐写

Bu

https://blog.csdn.net/qq_43431158

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII	
00	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG		IHDR
10	00	00	01	F4	00	00	01	A4	08	06	00	00	00	CB	D6	DF	ô	█	EOB
20	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	š	oHYS	t

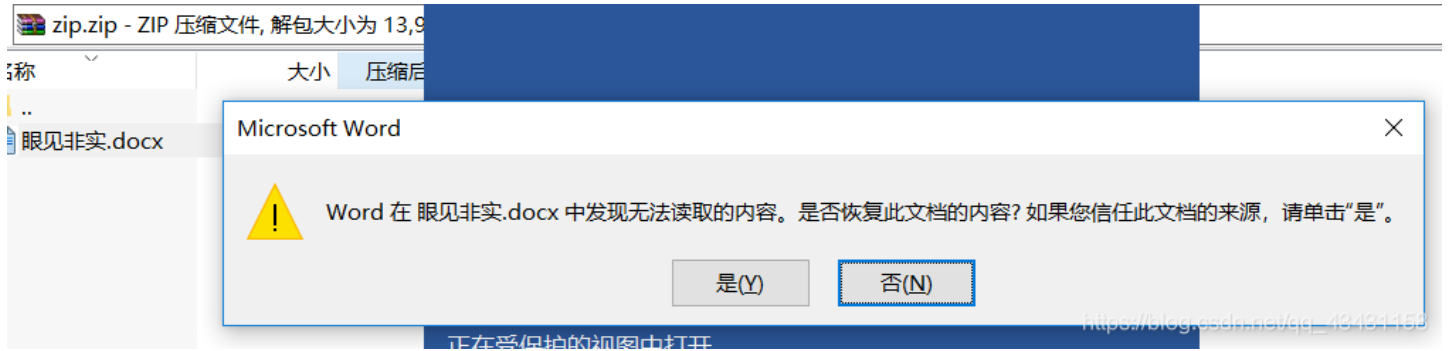
前四位是宽度，后四位是高度。将 A4修改位F4 即可得出flag

telnet

winhex打开就可得出flag

```
17 46 01 D4  "À" "Ù" "€" "À" "Ù" "z" "F" "Ó"
20 66 6C 61  Nhø*zP <· fla
31 62 66 39  g{d316759c281bf9
34 39 37 33  25d600be698a4973
20 00 00 3C  d5} >| < <
26 7F 0F 08  \ + \
```

眼见非实(ISCCCTF)



下载之后打不开, 根据提示眼见非实, 将 docx文件改成zip文件

名称	大小	压缩后	日期
theme		文件夹	2016/8/15 4:06
document.xml	1,912	661 XML 文档	1980/1/1 0:00 8B729375
fontTable.xml	1,552	521 XML 文档	1980/1/1 0:00 0CCEB45F

```
- <w:r>
  <w:t>在这里哟! </w:t>
</w:r>
</w:p>
<w:p w:rsidRDefault="002B3D8D" w:rsidR="002B3D8D" w:rsidRPr="002B3D8D">
  - <w:pPr>
    - <w:rPr>
      <w:rFonts w:hint="eastAsia"/>
      <w:vanish/>
    </w:rPr>
  </w:pPr>
  - <w:r w:rsidRPr="002B3D8D">
    - <w:rPr>
      <w:vanish/>
    </w:rPr>
    <w:t>flag{F1@g}</w:t>
  </w:r>
```

https://blog.csdn.net/qq_43431158

即可得出flag

啊哒

啊哒!



https://blog.csdn.net/qq_43431158

用winhex打开，发现隐藏有zip文件，用binwalk进行分离



得到一个加密文本，开始以为是伪加密，但用winhex打开后查看不是伪加密，因为不知道是否含字符、或是几位数，所以暴力破解也是不可取的，回去查看第一张照片，应该还隐藏有信息。



果然藏有东西，base16解码即可得出密码 `sdnisc_2018`，打开文本即可得出flag

又一张图片，还单纯吗



https://blog.csdn.net/qq_43431158

第一反应便是winhex打开，结果也没有发现什么，用binwalk分离也分离不出来，但确实能看出里面隐藏有文件。这里就需要一个新的工具 `foremost-master` 分离工具。

输入命令，提取出文件，即可得出flag

```
$ foremost -T 2.jpg
Processing: 2.jpg
|*|
```

00000000.jpg 00000310.jpg



00000000.jpg



00000310.jpg

猜

百度识图，直接可以识别是谁，至于flag提示中有

隐写2



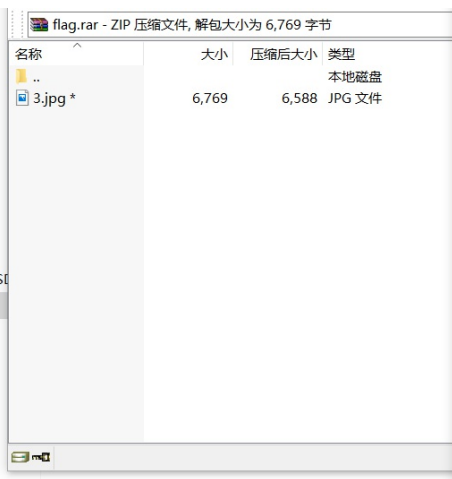
想拿到flag？心中ないいくつかB数かの？

https://blog.csdn.net/qq_43431158

winhex查看

```
E 7F mjàÜÿtyîÿžÿ ÿ:p
0 08 »ŒŒp PK ?
C 1A 8~nK*F÷NL L
0 00 $
0 00 flag.rar
3 01 /"$ jó
3 01 U $ jó U $ jó
E 4B PK ? ø}nK
4 00 t\ î Y äh $
```

binwalk进行分离



告诉你们一个秘密，密码是3个数哦。

查理曼：

查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。

雅典娜：

女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。

兰斯洛特，

英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。

Hint:

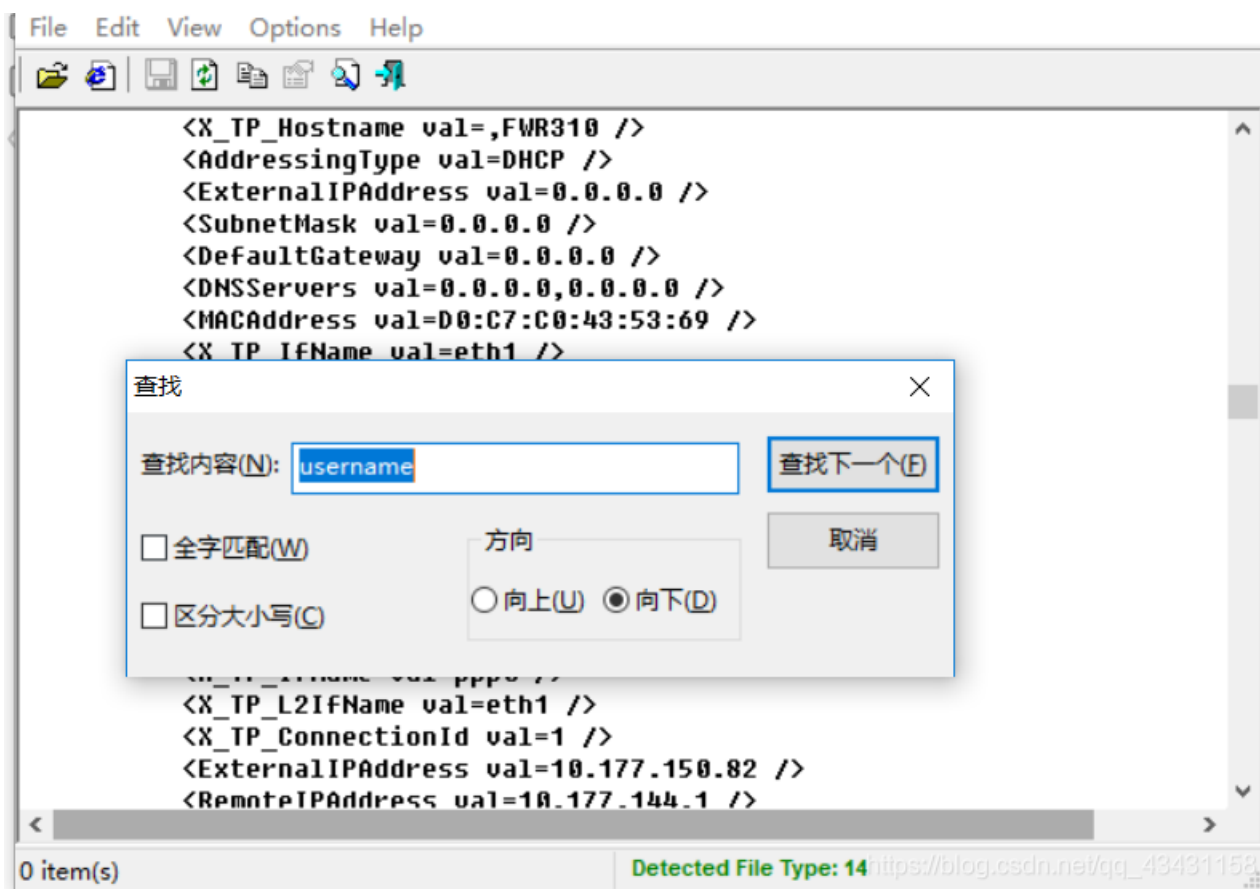
分离出一个加密的图片，和一个提示，既然都告诉了我们密码是3个数，直接暴力破解密码为 871，即可得出flag

宽带信息泄露

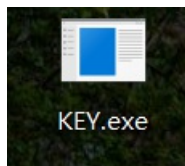


一开始各种方法都试过，实在没思路，回去看题目，宽带信息泄露，用文本打开是乱码，说明被加密了，这里就需要一个工具 RouterPassView 来帮助做题了

又提示 flag{宽带用户名}，打开工具直接查找username，即可得出flag。



多种方法解决



用winhex打开后，发现是base64转图片的格式，在线转图片，即可得出flag

图片转换Base64 在线把图片转换成Base64

点击这里选择选择要转换成Base64的图片 复制 清空

```
/rm9eGEuUksN7g3SepMjbZPuP90X9+8PpwwN0mb72pYfzcn1rf8NHwffXXWhxPmJmzXQ3r7+bE+pafhu+jr876cMLC  
JG2+q2H93ZxY3/LT8H301VkfTpibpM13Nay  
/mxPrW34avo++OuvDCXOT7OZGu7e+5YT9XynlhH36DlfvftcJLu50e6tbzlhf1diOWGfvsPVux8xN8lubrR761tO2N+V  
WE7Yp+9w9e5HzE2ymxvt3vqWE/Z3JZYT9uk7XL1+1GD3LX8avt8klhu2t5yc6F+/68OT2H3Ln4bvN4nlhu0tJyf61+  
/68CR23/Kn4ftNYrlhe8vJif71uz48id23/Gn4fpNYbtjecnKif  
/3+++HTnub0fd4zieUtlfrO1y9PH7K05y+z3smsbyF93Z9h6uXx095mtP3ec8klrfw3q7vcPXy+CIPc/o+75nE8hbe2  
/Udzv9X+sv/OP/881/SqtvcdpBh+wAAAABJRU5ErkJggg==
```

还原生成的Base64编码为图片:





https://blog.csdn.net/qq_43431158

得出一个gif二维码，用神器**Stegsolve**即可得出18张二维码图片，扫码即可得出flag





https://blog.csdn.net/qq_43431158

一开始用winhex打开，没有注意到末尾，尝试了其他方法不行才发现末尾的重要信息。

2FD0	74 F7 4B 65 B0 58 2F 01 3A 92 BF 1E 73 2A C7 49	t÷Ke°X/ : ' ¿ s*ÇI
2FE0	E6 03 A7 9D 14 11 1D 79 D0 9D 28 0E A5 1D 40 20	æ \$ yÐ (¥ @
2FF0	78 DC 59 69 DA 8F 64 6E E6 7B A3 57 31 EE 8D DC	xÜYiÚ dnæ{£Wlî Û
3000	CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67	ËbEb%î [Ü¶s äÿÜfg
3010	32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77	2ivyo}l{2s3_o@aw
3020	5F 5F 72 63 6C 40	_rcl@

这里可以看到 flag 只是顺序被打乱了，栅栏加密，解密即可得出flag

```
fg2ivyo}l{2s3_o@aw__rcl@
```

每组字数

```
flag{w22 is v3ry cool}@@
```

https://blog.csdn.net/qq_43431158

flag 需去除两个@

隐写3



https://blog.csdn.net/qq_43431158

这道题要敏感，大白怎么可能光一个头，所以应该是改图片的宽高，即可得出flag

89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG	IHDR	
00	00	02	A7	00	00	02	A7	08	06	00	00	00	6D	7C	71	\$	\$	m q
35	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	5	sRGB	@i é



https://blog.csdn.net/qq_43431158

这样才可爱

爆照(08067CTF)



下载图片，用winhex打开后发现隐藏着zip文件，binwalk进行分离。

本地磁盘					
8	92,278	8,362	文件	2017/10/28 1:...	08B388EA
88	15,739	14,906	文件	2017/10/28 1:...	A756F515
888	18,479	11,129	文件	2017/10/28 1:...	76D00172
8888	11,782	10,371	文件	2017/10/28 2:...	06601D...
88888	92,278	6,945	文件	2017/10/28 1:...	42B9AAFB
888888	92,278	6,824	文件	2017/10/28 1:...	1AC014...
8888888	92,278	7,076	文件	2017/10/28 1:...	6F836171
88888888	92,278	8,219	文件	2017/10/28 1:...	2BDC3B31
愉快的排序吧哈...	58,893	52,997	GIF 文件	2017/10/28 1:...	08F0DF8D

给了一堆文件，把后缀名改为jpg,看看能显示出什么



发现其中一个有二维码，扫出 **bilibili**

再看题目提示答案格式

flag格式 flag{xxx_xxx_xxx}

我们应该还漏掉有其他答案，再回去查看图片



属性	值
说明	
标题	
主题	
分级	☆☆☆☆☆
标记	
备注	c2lsaXNpbGk=

888.jpg发现base64, 解密得出 `silisili`

应该还有一个

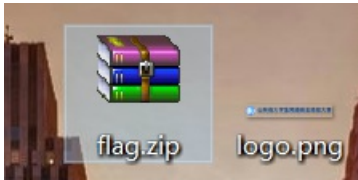
在8888.jpg中发现隐藏有图片, binwalk一下即可

00002D00	E3 57 CC 85 AE A2 7B AE 68 C3 E3 BB D3 ED A3 12	asmyopu)E-W zE)U
00002D70	AA CA 6A 74 AD C0 F6 60 34 42 74 55 C3 A5 A1 FF	ãwì...@ç{hÃã»Óí£
00002D80	D9 3D 00 76 84 02 00 00 B2 04 00 00 0E 00 24 00	^Êjt-Àö`4BtUÃ¥;ÿ
00002D90	00 00 00 00 00 00 20 00 00 00 00 00 00 00 31 35	PK ? É \K
00002DA0	00 00 00 00 01 00 18 00 1C 14 54 7D 4B 4F D3 01	Ù= v,, º \$
00002DB0	2C 60 39 7D 4B 4F D3 01 2C 60 39 7D 4B 4F D3 01	15
00002DC0	50 4B 05 06 00 00 00 01 00 01 00 60 00 00 00	09126368.png
00002DD0	B0 02 00 00 00 00	T}KOÓ
00002DE0		,`9}KOÓ ,`9}KOÓ
00002DF0		PK
00002E00		

得出 `panama`

按照题目提示拼接成flag即可

神秘的文件



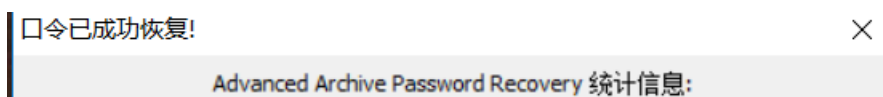
flag压缩包中还有一个logo图片

名称	大小	压缩后大小	类型	修改时间	CRC32
本地磁盘					
2018山东省大...	272,070	259,726	Microsoft Word ...	2018/11/2 14:...	6C5C9C45
logo.png *	27,870	27,405	PNG 文件	2018/10/15 1...	3E62BF64

明文攻击, 把外面的logo图片也压缩进flag压缩包中

名称	大小	压缩后大小	类型	修改时间	CRC32
本地磁盘					
1.png	27,870	27,393	PNG 文件	2018/10/15 1...	3E62BF64
2018山东省大...	272,070	259,726	Microsoft Word ...	2018/11/2 14:...	6C5C9C45
logo.png *	27,870	27,405	PNG 文件	2018/10/15 1...	3E62BF64

接下来爆破口令



总计口令	n/a
总计时间	15s 289ms
平均速度(口令/秒)	n/a
这个文件的口令	q1w2e3r4
十六进制口令	71 31 77 32 65 33 72 34

保存... 确定

https://blog.csdn.net/qq_43431158

打开word



哪有什么 WriteUP，别想了，老老实实做题吧！

https://blog.csdn.net/qq_43431158

既然找不到flag，把你变成zip格式看看是否隐藏有

2018山东省大学生网络安全技能大赛决赛writeup.zip (评估版)

文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)

添加 解压到 测试 查看 删除 查找 向导 信息 扫描病毒 注释 自解压格式

2018山东省大学生网络安全技能大赛决赛writeup.zip\docProps - ZIP 压缩文件, 解包大小为 309,168 字节

名称	大小	压缩后大小	类型	修改时间	CRC32
..			本地磁盘		
app.xml	695	362	XML 文档	1980/1/1 0:00	9ACE90AE
core.xml	773	387	XML 文档	1980/1/1 0:00	837797CF
flag.txt	32	34	文本文档	2018/11/2 14:...	FE2B014F
thumbnail.jpeg	36,452	36,452	JPEG 文件	1980/1/1 0:00	E5BD8199

https://blog.csdn.net/qq_43431158

找到了

flag.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

ZmxhZ3tkMGNYXzFzX3ppUF9maWxlfQ==

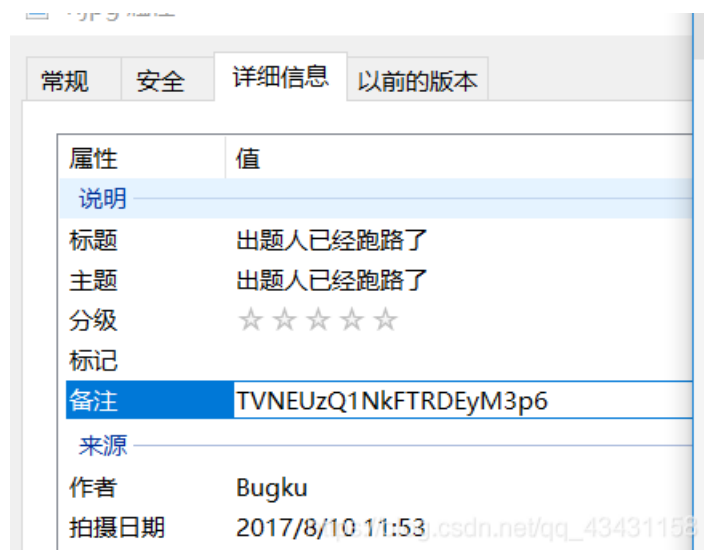
base64解密即可得出flag

细心的大象



https://blog.csdn.net/qq_43431158

细心的大象，要细心，看看照片详细信息隐藏有东西没



果然，这个又是 base64 加密的

接下来，把照片 binwalk 一下，出来一个压缩包，里面一个加密的图片





上面base64解密后的密码就是这个照片的密码

Bu

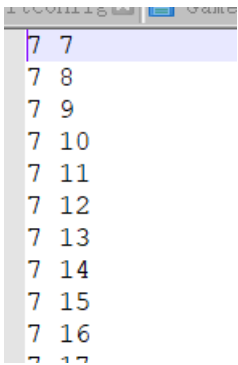
https://blog.csdn.net/qq_43431158

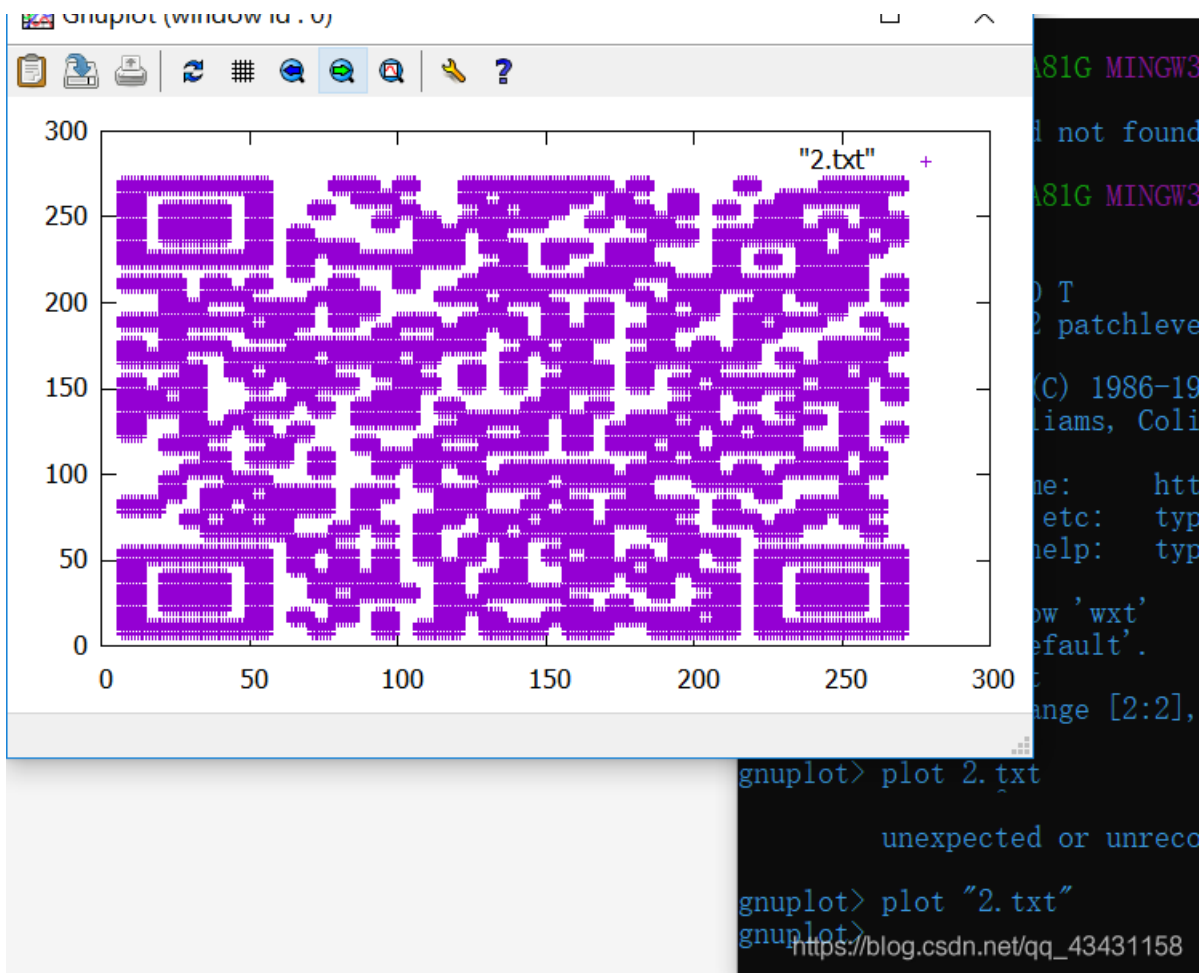
跟一开始遇到那道题一样，修改宽高即可得出flag

图穷匕见



之前做过这种题，打开winhex后发现一堆十六进制，在 notepad++ 打开后转成ascii，再替换成相应的格式即可画图。





具体做法这里就不细说了，之前总结的也做过这个题。

这次就先总结到这里，另一部分的题写到下一篇博客中。