

# 图片隐写题解第二弹

原创

[huster0828](#) 于 2020-11-18 19:25:06 发布 351 收藏 4

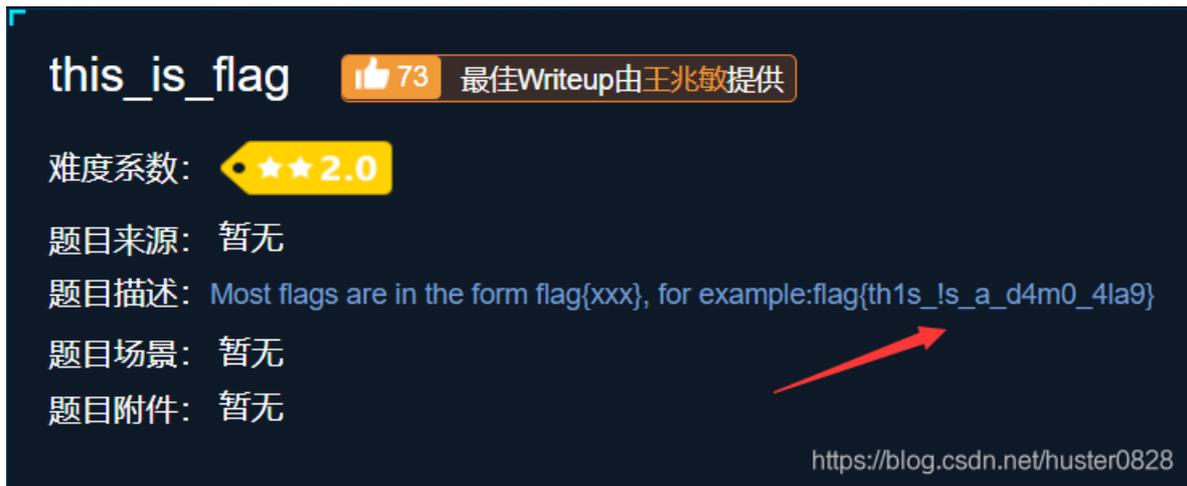
版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/huster0828/article/details/109683022>

版权

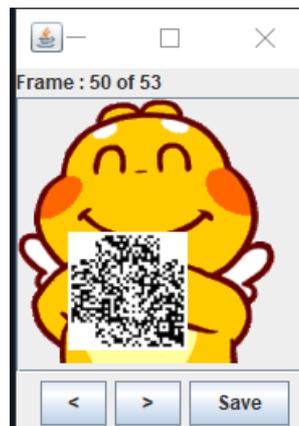
## 1.this\_is\_flag(from攻防世界)

这道题没有附件，这道题就是在题目中的！



## 2.give\_you\_flag(from攻防世界)

里面有一个gif，在后面闪过一个二维码，然后用stegsolve->Analyse->Frame Browser就能看到一帧一帧的图片啦，然后就找到了一个二维码



可是缺二维码定位的东西，所以我们要把他P上



然后就出来啦。不过这个要多扫一下，我最开始都扫不出来，用朋友的手机才扫出来的

### 3. 眼见非实 (from Bugku)

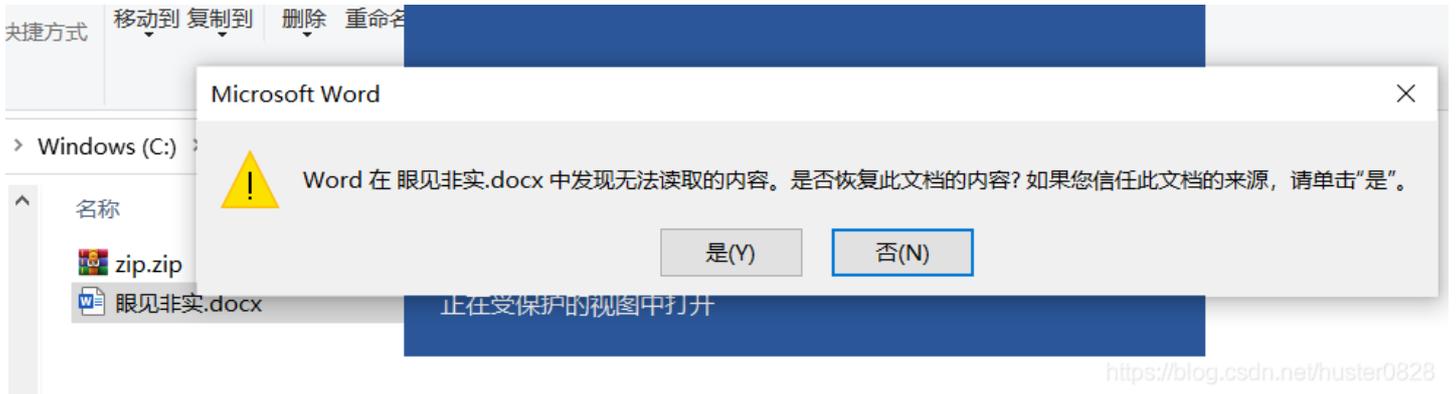
下载下来是一个名为zip的文件

名称	修改日期
zip	2020/11/17 14:38

用file查看后是zip压缩包，然后我们改一下后缀

```
huster@LAPTOP-4J27RSD4:/mnt/c/study$ file zip
zip: Zip archive data, at least v2.0 to extract
huster@LAPTOP-4J27RSD4:/mnt/c/study$
```

解压后实一个.docx的word文档，发现打不开



<https://blog.csdn.net/huster0828>

然后我又用file查看了文件的属性，结果发现这其实是一个压缩包

```
huster@LAPTOP-4J27RSD4:/mnt/c/study$ ls
zip.zip  眼见非实.docx
huster@LAPTOP-4J27RSD4:/mnt/c/study$ file 眼见非实.docx
眼见非实.docx: Zip archive data, at least v1.0 to extract
huster@LAPTOP-4J27RSD4:/mnt/c/study$
```

解压之后是一个文件夹

名称	修改日期	类型	大小
_rels	2016/8/15 4:06	文件夹	
customXml	2016/8/15 4:06	文件夹	
...	2016/8/15 4:06	文件夹	

docProps	2016/8/15 4:06	文件夹	
word	2016/8/15 4:06	文件夹	
[Content_Types].xml		XML 文档	2 KB

<https://blog.csdn.net/huster0828>

然后在word中的document中发现了可疑之处

名称	修改日期	类型	大小
_rels	2016/8/15 4:06	文件夹	
theme	2016/8/15 4:06	文件夹	
document.xml		XML 文档	2 KB
fontTable.xml		XML 文档	2 KB
settings.xml		XML 文档	3 KB
styles.xml		XML 文档	29 KB
webSettings.xml		XML 文档	1 KB

<https://blog.csdn.net/huster0828>

然后就找到flag啦

```

- <w:p w:rsidRDefault="002B3D8D" w:rsidR="002B3D8D">
  - <w:r>
    <w:t>Flag</w:t>
  </w:r>
  - <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>
  <w:bookmarkStart w:name="_GoBack" w:id="0"/>
  <w:bookmarkEnd w:id="0"/>
</w:p>
- <w:sectPr w:rsidR="002B3D8D" w:rsidRPr="002B3D8D">

```

<https://blog.csdn.net/huster0828>

#### 4. 隐写3(from Bugku)

下载下来是一张图片



这不一看就少了半截，然后再winhex里修改一下,然后就出来啦

t	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	+
10	00	00	02	A7	00	00	02	A7	08	06	00	00	00	6D	7C	71	.
20	35	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	5
30	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	.
40	00	09	70	48	59	73	00	00	0E	C4	00	00	0E	C4	01	95	.
50	2B	0E	1B	00	00	FF	A5	49	44	41	54	78	5E	EC	BD	07	+



## 5. 分解1(from whale)

```
binwalk: command not found
huster@LAPTOP-4J27RSD4:/mnt/c/study/1$ binwalk 02.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
382         0x17E      Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"
3192        0xC78     TIFF image data, big-endian, offset of first image directory: 8
140147     0x22373   JPEG image data, JFIF standard 1.01
140177     0x22391   TIFF image data, big-endian, offset of first image directory: 8
huster@LAPTOP-4J27RSD4:/mnt/c/study/1$
```

<https://blog.csdn.net/huster0828>

分离之后，就找到flag啦



00000000.jpg



00000273.jpg

## 6. 下雨天(from whale)

用binwalk查看之后发现是有一张动图

```
huster@LAPTOP-4J27RSD4:/mnt/c/study/2$ binwalk rain.jpg
DECIMAL      HEXADECIMAL     DESCRIPTION
-----
0            0x0             GIF image data, version "89a", 498 x 768
huster@LAPTOP-4J27RSD4:/mnt/c/study/2$ \
```

然后我将后缀名改了之后，用Stegsolve一帧一帧的看



然后就找到flag啦

## 7. 分解2(from whale )

binwalk之后发现还有这么多图片，然后再分离一下

```
huster@LAPTOP-4J27RSD4:/mnt/c/study/3$ binwalk 03.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.02
30	0x1E	TIFF image data, big-endian, offset of first image directory: 8
332	0x14C	JPEG image data, JFIF standard 1.02
8817	0x2271	JPEG image data, JFIF standard 1.02
301910	0x49B56	JPEG image data, JFIF standard 1.01

<https://blog.csdn.net/huster0828>

然后就分离出flag啦~



00000000.jpg



00000589.jpg

<https://blog.csdn.net/huster0828>

## 8. 分解3 (from whale)

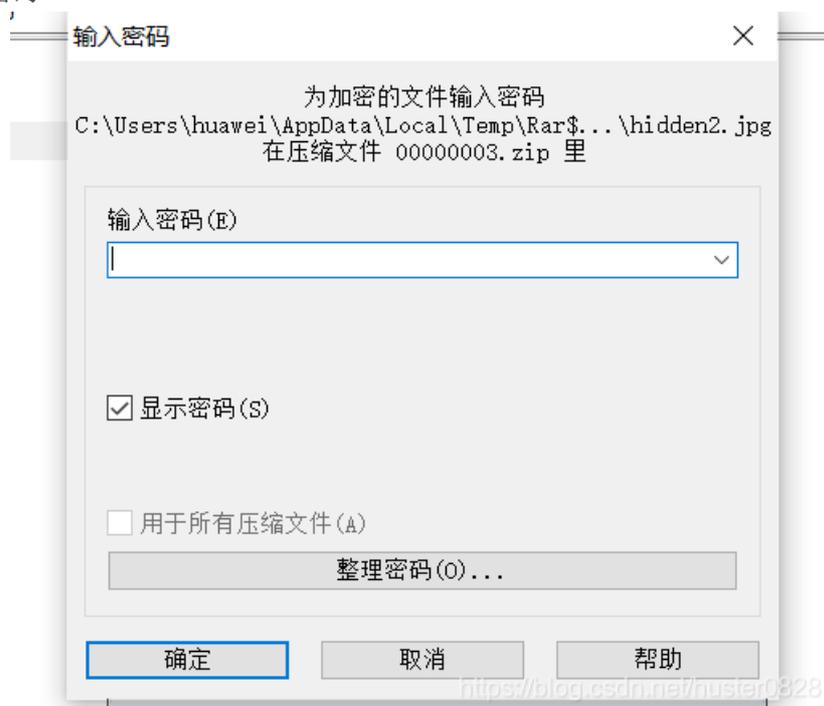
binwalk之后发现里面的东西也有一点多，然后再分离一下

```
huster@LAPTOP-4J27RSD4:/mnt/c/study/4$ binwalk hidden.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 351 x 560, 8-bit/color RGBA, non-interlaced
41	0x29	Zlib compressed data, default compression
1975	0x7B7	Zip archive data, at least v1.0 to extract, compressed s
1742, name: hidden2.jpg		
293851	0x47BDB	End of Zip archive, footer length: 22

<https://blog.csdn.net/huster0828>

里面有个压缩包打开需要密码



然后还有分离出来的图片



一直试着把压缩包的密码找到，结果怎么输入都不对，最后直接将图中的flag输进去了，然后就对啦~

## 9. 女神(from whale)

binwalk之后就是一张普通的jpg图片

```
huster@LAPTOP-4J27RSD4:/mnt/c/study/5$ binwalk goddess.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01

用记事本打开之后，再末尾就找到flag啦

```
ï¸?d稗餹邨?鉞鐘 ?H嫩?*考j J壘□雋鬪  
ÿ霜| l e妘□+d獸W?□U鼻Jm□缘□D ?□□  
温 寘lag:nctf{pic_yin_xie_shu}
```

### 10. 捉迷藏(from whale)

```
huster@LAPTOP-4J27RSD4:/mnt/c/study/1$ binwalk password.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 600 x 108, 8-bit/color RGB, non-interlaced
62	0x3E	Zlib compressed data, default compression

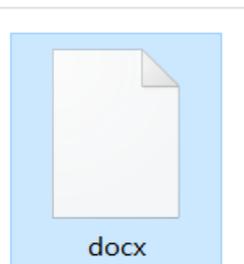
貌似有点问题，然后分离，分离出来就是一张照片，但是里面肯定藏着什么

用stegsolve打开，再random colour map3找到flag啦



### 11. word隐写(from whale)

这道题就是word的隐写



打不开，然后用file查看一下

```
huster@LAPTOP-4J27RSD4:/mnt/c/study/2$ file docx  
docx: Microsoft Word 2007+
```

然后改一下后缀名，打开之后就是这种

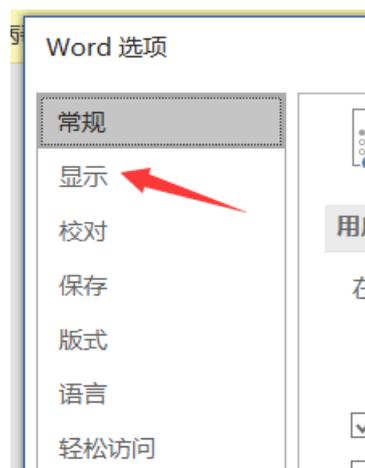


锦带书十二月启·林钟六月

伏渐终，  
夏将谢。  
飞腐草，光浮帐里之书；  
噪繁柯，影入机中之鬓。  
枝迁而潦溢，  
槿茂而发荣。  
土焦而流金，  
水沸而漂烁。  
想足下，  
形月府，  
迹冰床。  
庄子之七篇，逍遥物外；  
老明之两卷，恍惚怀中。  
某白社狂人，  
缙末学，  
从州县之职，  
立松鹤之闲，  
假德以为邻，  
借书而取友。  
千年之独鹤，暂逐鸡群；  
万里之孤鹏，权潜燕侣。  
非得意，正可忘言。  
不具伸，应俟面会。

<https://blog.csdn.net/huster0828>

word的隐写首先查看它有没有隐藏字符





### 页面显示选项

- 在页面视图中显示页面间空白(W) ⓘ
- 显示突出显示标记(H) ⓘ
- 悬停时显示文档工具提示(L)

### 始终在屏幕上显示这些格式标记

- 制表符(T) →
- 空格(S) ...
- 段落标记(M) ↵
- 隐藏文字(D) abc
- 可选连字符(Y) ~
- 对象位置(C) ⚓
- 可选分隔符(O) ¶
- 显示所有格式标记(A)

然后每一行后面就是flag啦！

←  
 锦带书十二月启·林钟六月←  
 ←  
 伏渐终, v←  
 夏将谢, e←  
 飞腐草, 光浮帐里之书; n←  
 噪繁柯, 影入机中之鬓。 u←  
 枝迁而潦溢, s←  
 槿茂而发荣。 c←  
 土焦而流金, t←  
 水沸而漂烁。 f←  
 想足下, {←  
 形月府, e←  
 迹冰床。 3←  
 庄子之七篇, 逍遥物外; j←  
 老明之两卷, 恍惚怀中。 N←  
 某白社狂人, n←  
 缙末学, i←  
 从州县之职, 2←  
 立松鹤之闲, 5←  
 假德以为邻, 2←  
 借书而取友。 j←  
 千年之独鹤, 暂逐鸡群; n←  
 万里之孤鹏, 权潜燕侣。 X←

非得意，正可忘言。  
不具伸，应俟面会。

<https://blog.csdn.net/huster0828>

## 12. 普通的二维码(from Bugku)

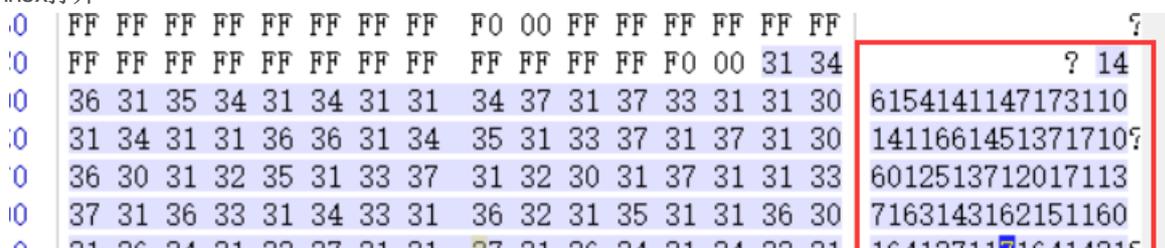
这个解压之后就是一个二维码



然后扫码之后是这个



然后用winhex打开



```

0 31 30 34 31 33 37 31 31 37 31 30 34 31 34 33 31 1041371110414317
:0 33 37 31 32 34 31 35 37 31 33 37 31 32 34 31 34 3712415713712414
:0 35 31 35 36 31 33 37 31 30 31 31 36 33 31 34 33 5156137101163143
:0 31 35 31 31 35 31 30 34 31 31 37 35 40 78 6A 73 151151041175@xjs
:0 65 63 6B 21 eck!

```

<https://blog.csdn.net/huster0828>

观察发现没有8和9，所以怀疑是8进制

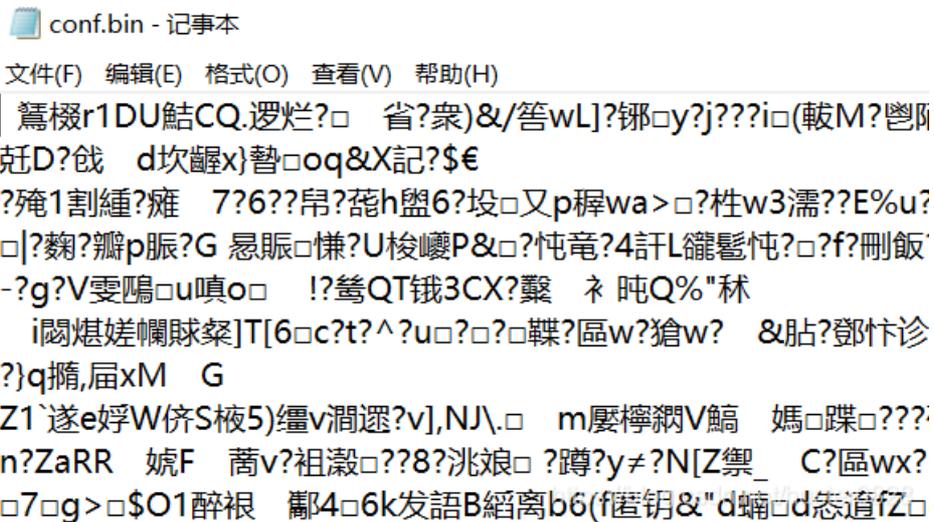
每三个为一组的八进制转换成十进制，然后十进制对照着ascii码，然后就有flag啦

**flag{Have\_y0U\_Py\_script\_Otc\_To\_Ten\_Ascii!}**

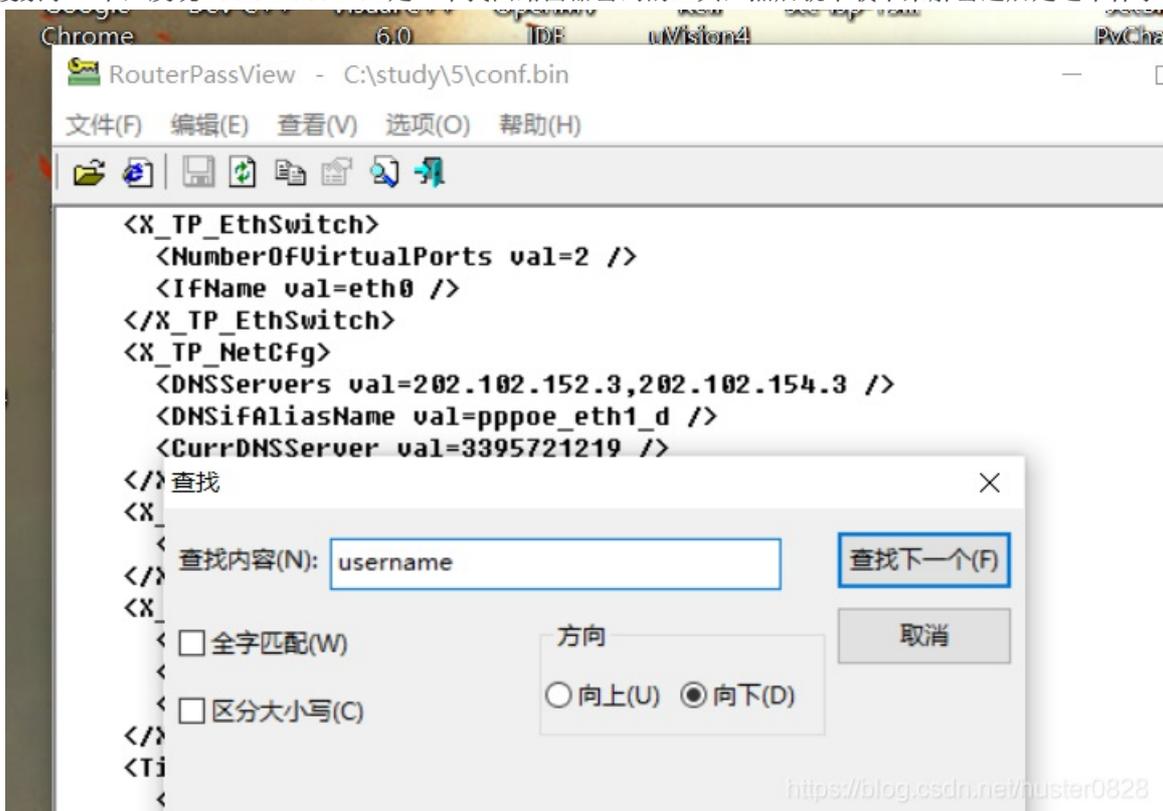
### 13. 宽带信息泄露(from Bugku)

下载之后用记事本打开，发现这可能是加密过后的文件

![在这里插入图片描述](https://img-blog.csdnimg.cn/20201118151516974.png#pic\_center)



然后在网上搜索了一下，发现RouterPassView是一个找回路由器密码的工具，然后就下载下来解密过后是这个样子



<https://blog.csdn.net/huster0828>

搜索用户名,然后就找到flag啦

```
<DefaultGateway val=10.177.144.1 /
<Name val=pppoe_eth1_d />
<Uptime val=671521 />
<Username val=053700357621 />
<Password val=210265 />
<X_TP_IfName val=ppp0 />
<X_TP_L2IfName val=eth1 />
<X_TP_ConnectionId val=1 />
```

#### 14. 多种方法解决(from Bugku)

下载下来是一个zip的压缩包，解压之后是一个.exe的运行程序，但是打不开

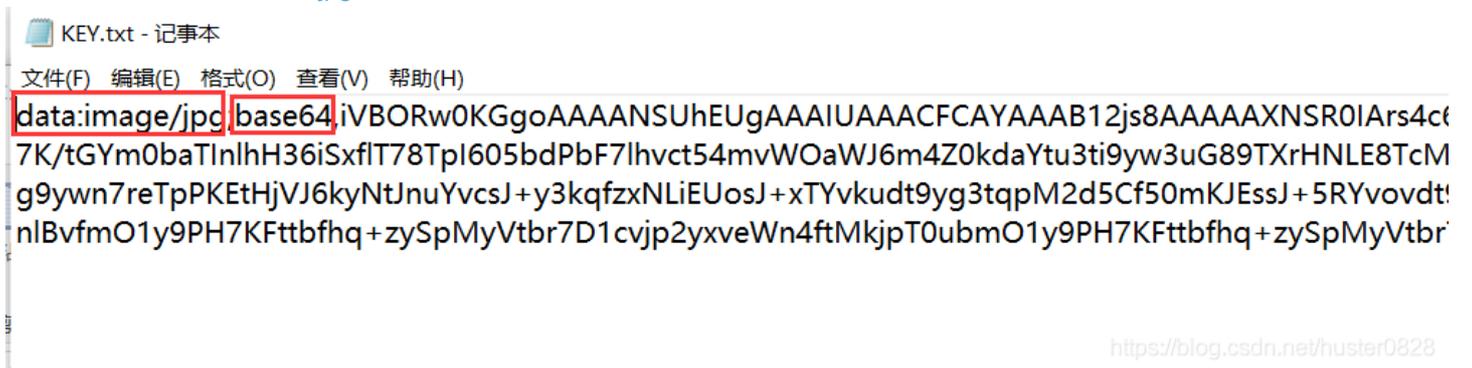


我将它改成jpg,但是打不开

KEY.jpg  
似乎不支持此文件格式。

<https://blog.csdn.net/huster0828>

然后将它改成txt,然后发现了jpg的图片和base64编码



<https://blog.csdn.net/huster0828>

再根据题目说做题过程中会得到一个二维码



## 多种方法解决

60

在做题过程中你会得到一个二维码图片

<http://123.206.87.240:8002/misc/3.zip>

Flag

Submit

<https://blog.csdn.net/huster0828>

然后就找了把base64转换成图片的网站  
link.



以下是您的 Base64 代码所解码出来的图片，右键另存为保存图片。



返回

CN22 

<https://blog.csdn.net/huster0828>

再用QR识别一下二维码，就找到flag啦~

已解码数据 1:

位置:(15.6,10.5)-(203.3,10.5)-(15.6,199.7)-(203.3,199.5)

颜色正常, 正像

版本: 4

纠错等级:Q, 掩码:3

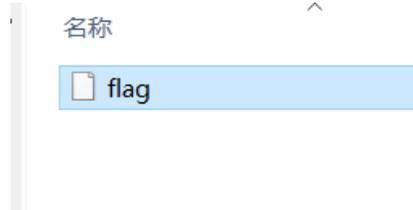
内容:

KEY{dca57f966e4e4e31fd5b15417da63269}

<https://blog.csdn.net/huster0828>

15. linux(from Bugku)

得到的是一个zip，解压过后里面有一个flag



用binwalk查看了一下发现是ext

```
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         Linux EXT filesystem,
data, UUID=66ce56f1-5b57-492f-82f3-ac0678797879
```

我用文件打不来，网上的大佬直接再命令行终端里搜索的

```
huster@LAPTOP-4J27RSD4:/mnt/c/study/6/test$ strings flag
[WI/
```

然后就找到flag啦

```
Path=game
#DeletionDate=2016-06-27T12:27:37
key {}
key {}
key {feb81d3834e2423c9903f4755464060b}
game.trashinfo
```

== strings 命令 ==

再对象文件或二进制文件中查找可打印的字符串

## 16. linux2(from Bugku)

查看文件格式是ext3,我不知道用啥打开，就改成了.txt

然后直接搜索KEY

```
娯鷗z??>g藥G0覲S??#} ?6p%?j?C?罈韜□?D敏吃
KEY{24f3627a86fc740a7f36ee2c7a1c124a}
```

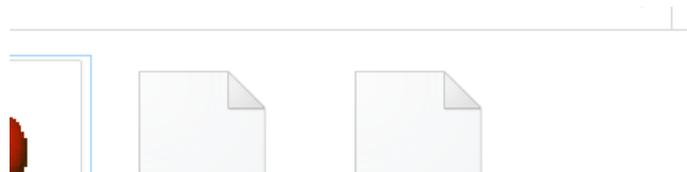
然后就找到了

## 17.come\_game(from Bugku)

下载下来是一个文件包，解压之后有一个游戏



玩了之后发现多出了几个文件





<https://blog.csdn.net/huster0828>

用winhex打开，发现32对应的是第二关

set	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0000	00	01	32	00	00	41	00	05	43	00	00	00	00	00	00	00	..2..A..C.....
0010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

然后我们改成35,然后就得到flag啦

joker's I wanna Medium SaveData1 [Esc]:end Death[1]:5 Time[1]:0:0:21



## 18. 做个游戏(from Bugku)

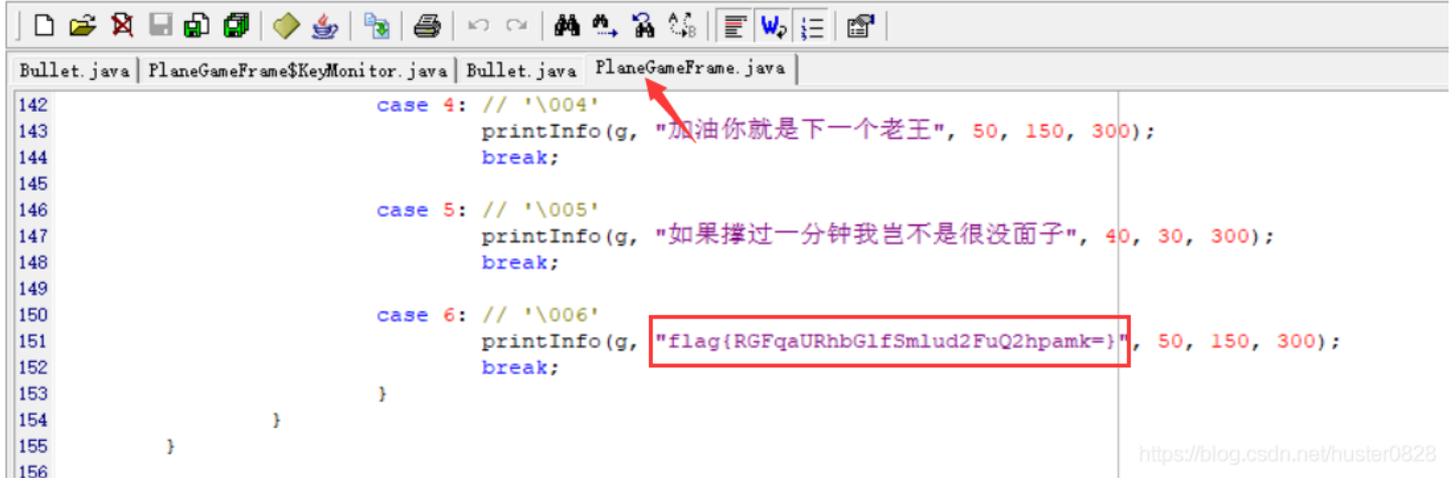
里面是一个.jar的游戏

heiheihei.jar

玩了好几次都过不了关，然后用反编译软件打开

XJad

文件(F) 编辑(E) 查看(V) 帮助(H)



```
142         case 4: // '\004'
143             printInfo(g, "加油你就是下一个老王", 50, 150, 300);
144             break;
145
146         case 5: // '\005'
147             printInfo(g, "如果撑过一分钟我岂不是很没面子", 40, 30, 300);
148             break;
149
150         case 6: // '\006'
151             printInfo(g, "flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}", 50, 150, 300);
152             break;
153     }
154 }
155 }
156
```

就找到flag啦，flag里面有=，应该使用base64加密

请将要加密或解密的内容复制到以下区域

DajiDali\_JinwanChiji

19. pdf(from 攻防世界)

打开是一个pdf，根据题目的提示

题目来源: [csaw](#)

题目描述: 菜猫给了菜狗一张图，说图下面什么都没有

说明图片下面有东西，然后用朗读此页内容，发现里面有隐藏的东西



然后pdf转为word文档



然后就找到flag啦，可以直接复制下来  
flag{security\_through\_obscurity}

## 20. 如来十三掌 (from 攻防世界)

打开是一个word文档

夜哆悉諳多苦奢陀奢諦冥神哆盧穆瞞三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉佉陀  
諳佈奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧瞞豆蒙密離佉婆瞞礙他哆提哆  
多鉢以南哆心日姪罰蒙呐神。舍切真佉勝呐得俱沙罰娑是佉遠得呐數罰輸哆遠薩得  
槃漫夢盧瞞亦醯呐娑瞞瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿瞞沙蘇  
輪奢恐百侄得罰提哆伽諳沙櫻鉢三死快摩大蘇老數一遮

看不懂，在网上搜了一下佛语加密，就出现了在线解密工具

## 与佛论禅帮助

将需要打码的文字输入在上面的文本框里，点击『听佛说宇宙的真谛』按钮，就能在下面得到打码后的文字。

将需要解码的文字输入在下面的文本框里，记得带上『佛曰：』或『如是我闻：』的文字，点击『参悟佛所言的真意』按钮，就能在上面的文本框里得到解码后的文字。

顺便说下，为什么有时候会出现『太深奥了，参悟不出佛经的真意.....』的情况，那是因为某些深井冰的网站（百度说的就是你！），会将繁体字转换为简体字，这样你复制后的文字已经不是最初的原文了，所以解不出。本佛祖的代言人已经尽力的去尝试参悟了，可惜还是有部分被篡改的佛语无能为力，十分抱歉o(>\_<)o

然也

## 与佛论禅

MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

本来无一物，何处惹尘埃

佛曰：夜哆悉諳多苦奢陀奢諦冥神哆盧穆瞞三徑三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智徑諸若奢數苦奢集遠俱老竟寫明奢若梵等盧瞞豆蒙密離怯婆瞞礙他哆提哆多鉢以南哆心曰姪罰蒙訥神。舍切真怯勝訥得俱沙罰娑是怯遠得訥數罰輸哆遠薩得槃漫夢盧瞞亦醯訥娑瞞瑟輸諳尼摩罰薩冥大倒參夢徑阿心罰等奢大度地冥殿瞞沙蘇輪奢恐豆徑得罰提哆伽諳沙楞鉢三死怯摩大蘇者數一遮

然后base64解密不了，再根据题目如来十三掌，猜测是ROT 1 3 解密

```
rot13
ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9
```

再base64解密，就得到flag啦

```
ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

flag{bdscjhbkmnfrdhbckijndskvbkjdsab}
```

<https://blog.csdn.net/huster0828>