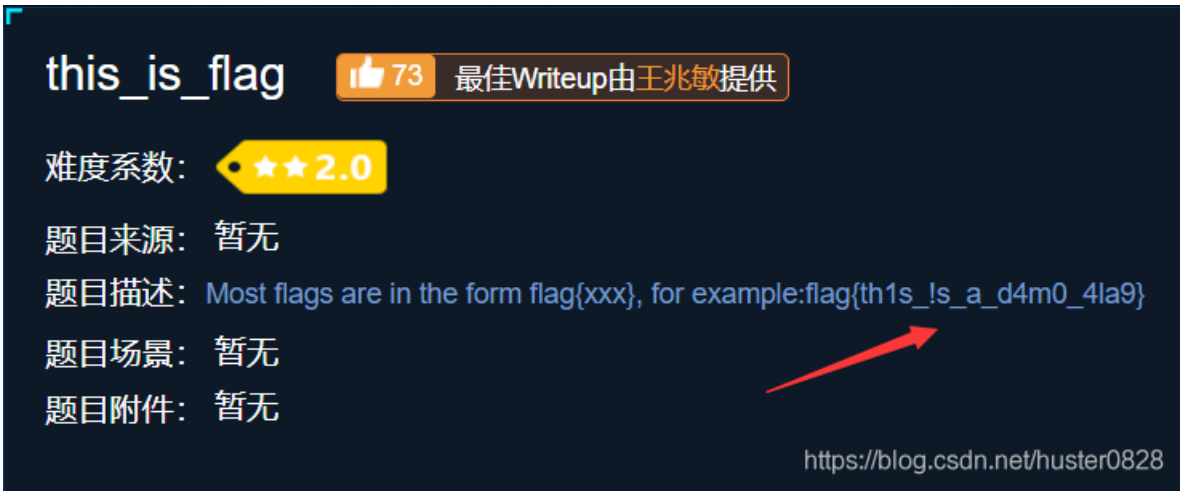
图片隐写题解第二弹

原创

huster0828 于 2020-11-18 19:25:06 发布

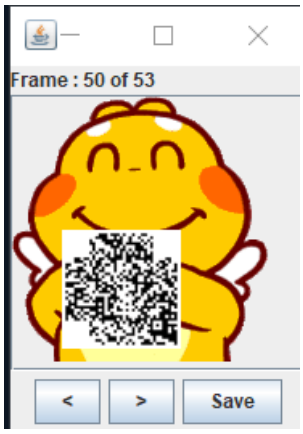
1.this_is_flag(from攻防世界)

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，在后面闪过了一个二维码，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

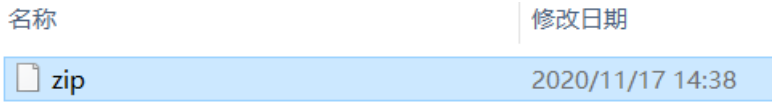


可是缺二维码定位的东西，所以我们要把他P上

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

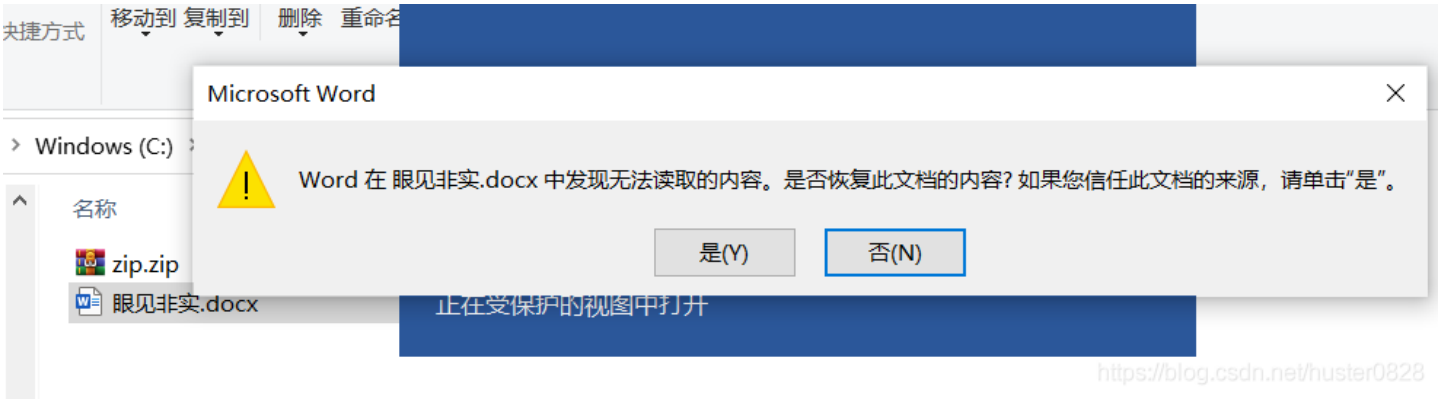
3. 眼见非实（from Bugku）

下载下来是一个名为zip的文件

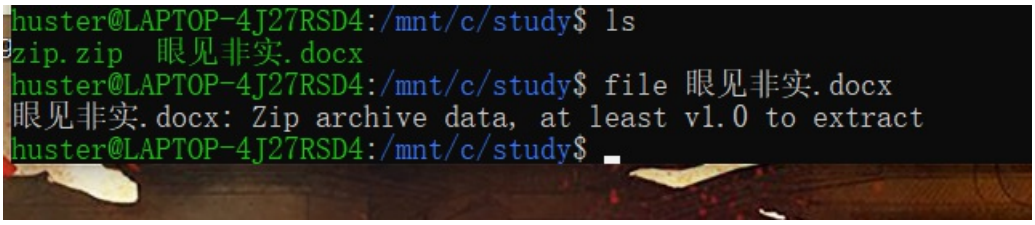


用file查看后是zip压缩包，然后我们改一下后缀

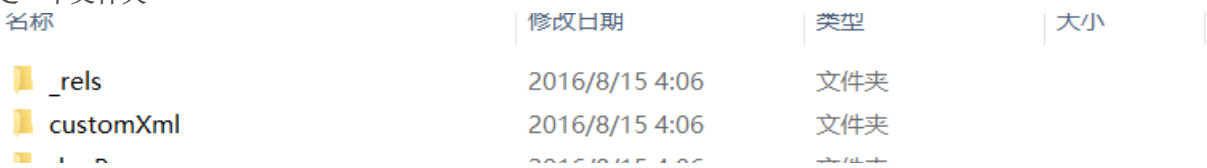
解压后实一个.docx的word文档，发现打不开

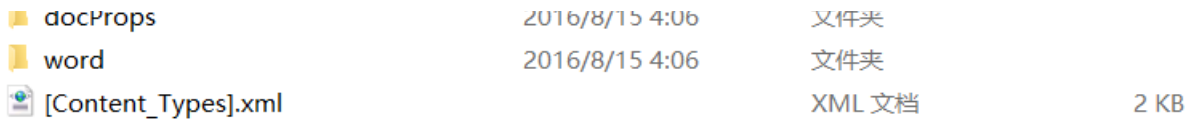


然后我又用file查看了这个文件的属性，结果发现这其实实一个压缩包

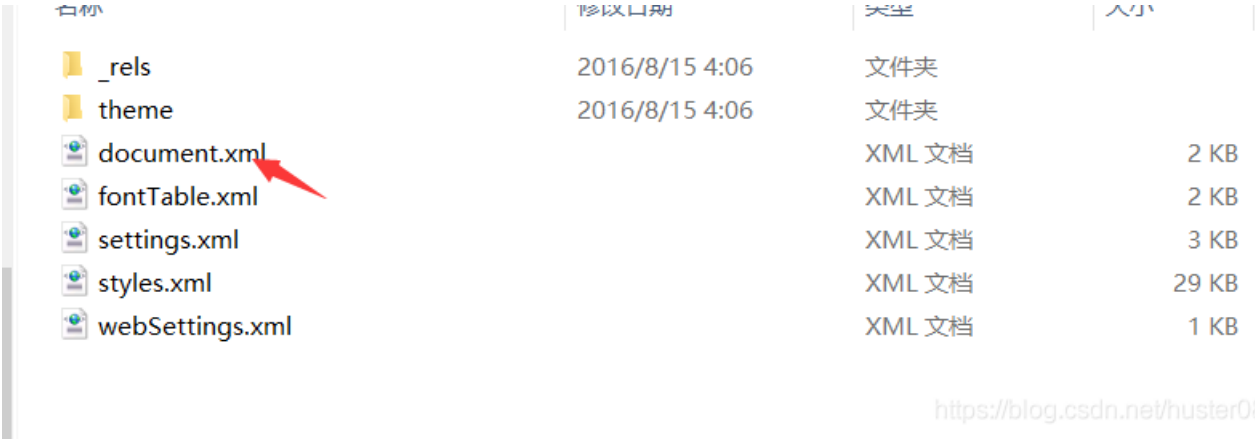


解压之后是一个文件夹





然后在word中的document中发现了可疑之处



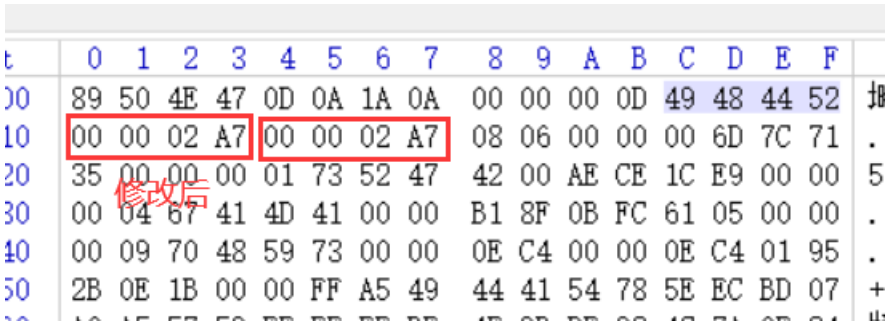
然后就找到flag啦

```
- <w:p w:rsidRDefault="002B3D8D" w:rsidR="002B3D8D">
  - <w:r>
      <w:t>Flag</w:t>
    </w:r>
  - <w:r>
      <w:t>在这里呦！</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:r>
  <w:bookmarkStart w:name="_GoBack" w:id="0"/>
  <w:bookmarkEnd w:id="0"/>
</w:p>
```


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



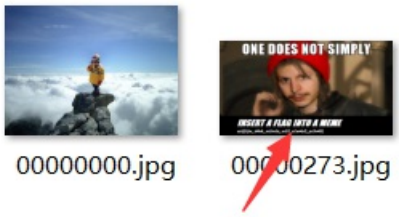
5. 分解1(from whale)

```
binwork: 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



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
```

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

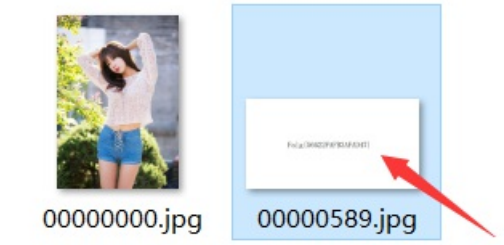
7. 分解2(from whale)

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
```


然后就分离出flag啦~



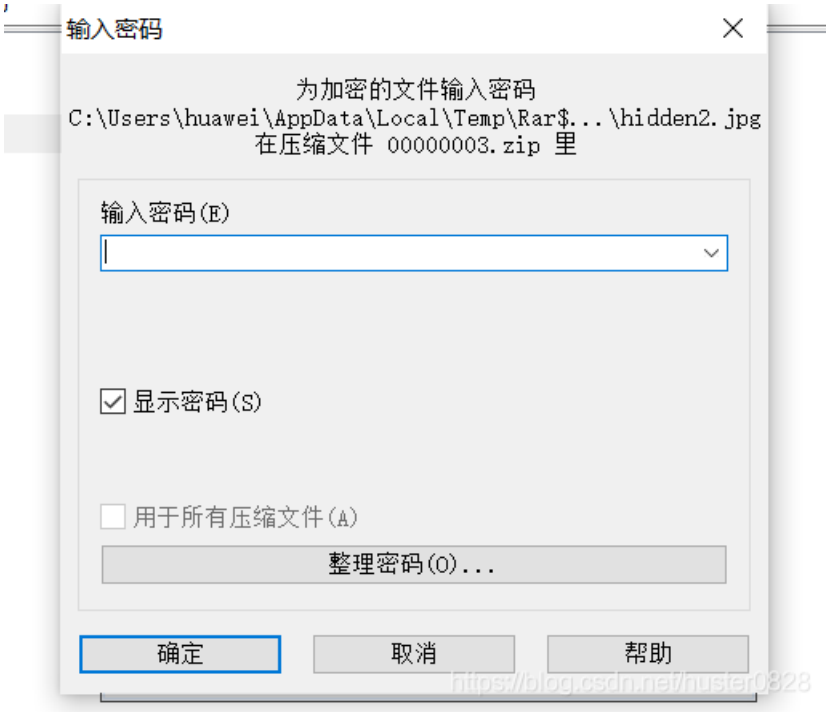
8. 分解3 (from whale)

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
```


里面有个压缩包打开需要密码

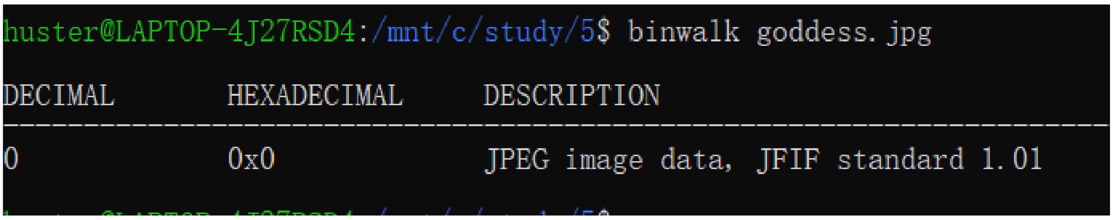


然后还有分离出来的图片

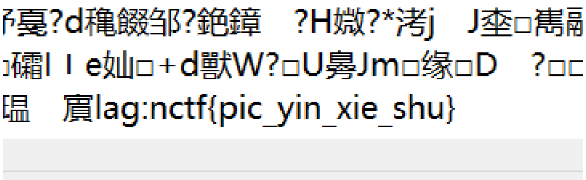
一直试着把压缩包的密码找到，结果怎么输入都不对，最后直接将图中的flag输进去了，然后就对啦~

9. 女神(from whale)

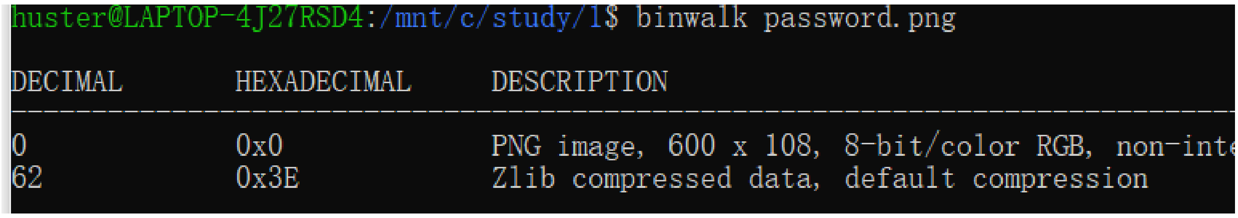
binwalk之后就是一张普通的jpg图片



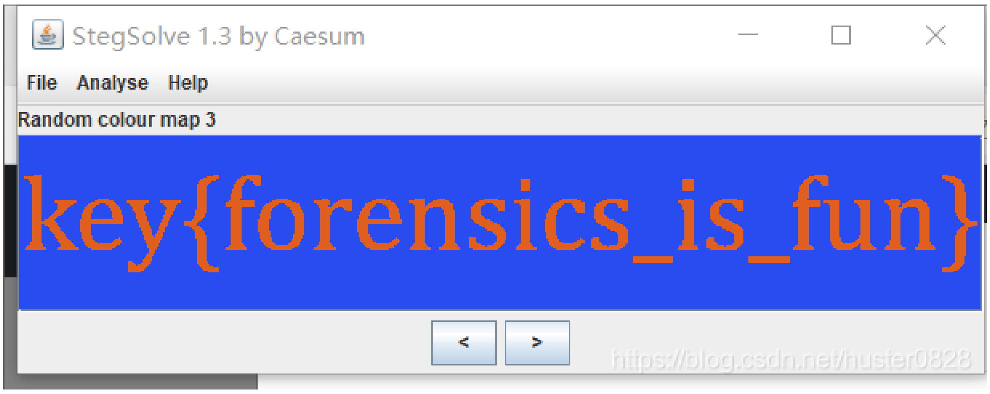
用记事本打开之后，再末尾就找到flag啦



10. 捉迷藏(from whale)

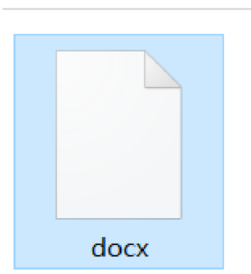


貌似有点问题，然后分离，分离出来就是一张照片，但是里面肯定藏着什么
用stegsolve打开，再random colour map3找到flag啦



11. word隐写(from whale)

这道题就是word的隐写



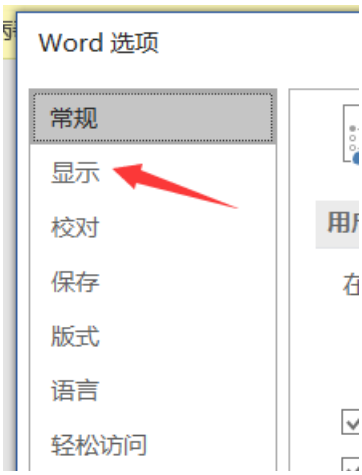
打不开，然后用file查看一下

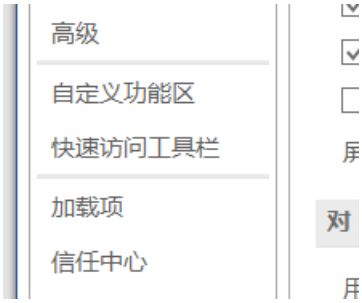
然后改一下后缀名，打开之后就是这种

锦带书十二月启·林锺六月

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，
缃末学，
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。

word的隐写首先查看它有没有隐藏字符





然后每一行后面就是flag啦！

锦带书十二月启·林锺六月

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；i
老明之两卷，恍惚怀中。N
某白社狂人，n
缃末学，i
从州县之职，2
立松鹤之闲，5
假德以为邻，2
借书而取友。i
千年之独鹤，暂逐鸡群；n
万里之孤鹏，权潜燕侣。X

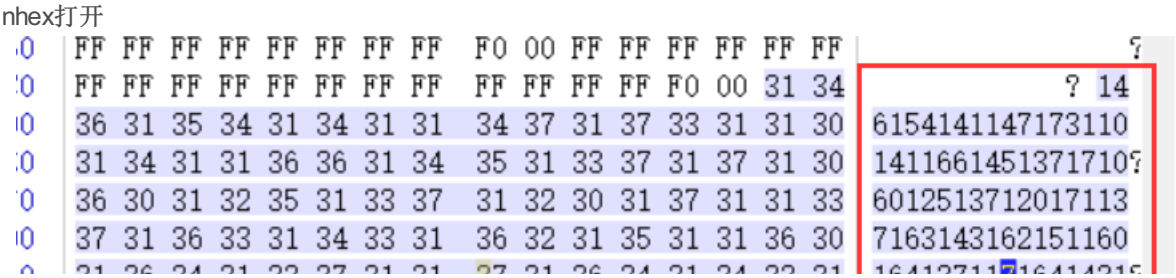
非得意，正可忘言。
不具伸，应俟面会。

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



```
31 36 34 31 33 37 31 31  37 31 36 34 31 34 33 31  16413711 16414317
33 37 31 32 34 31 35 37  31 33 37 31 32 34 31 34  3712415713712414
35 31 35 36 31 33 37 31  30 31 31 36 33 31 34 33  5156137101163143
31 35 31 31 35 31 30 34  31 31 37 35 40 78 6A 73  151151041175@xjs
65 63 6B 21                                       eck!
```

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

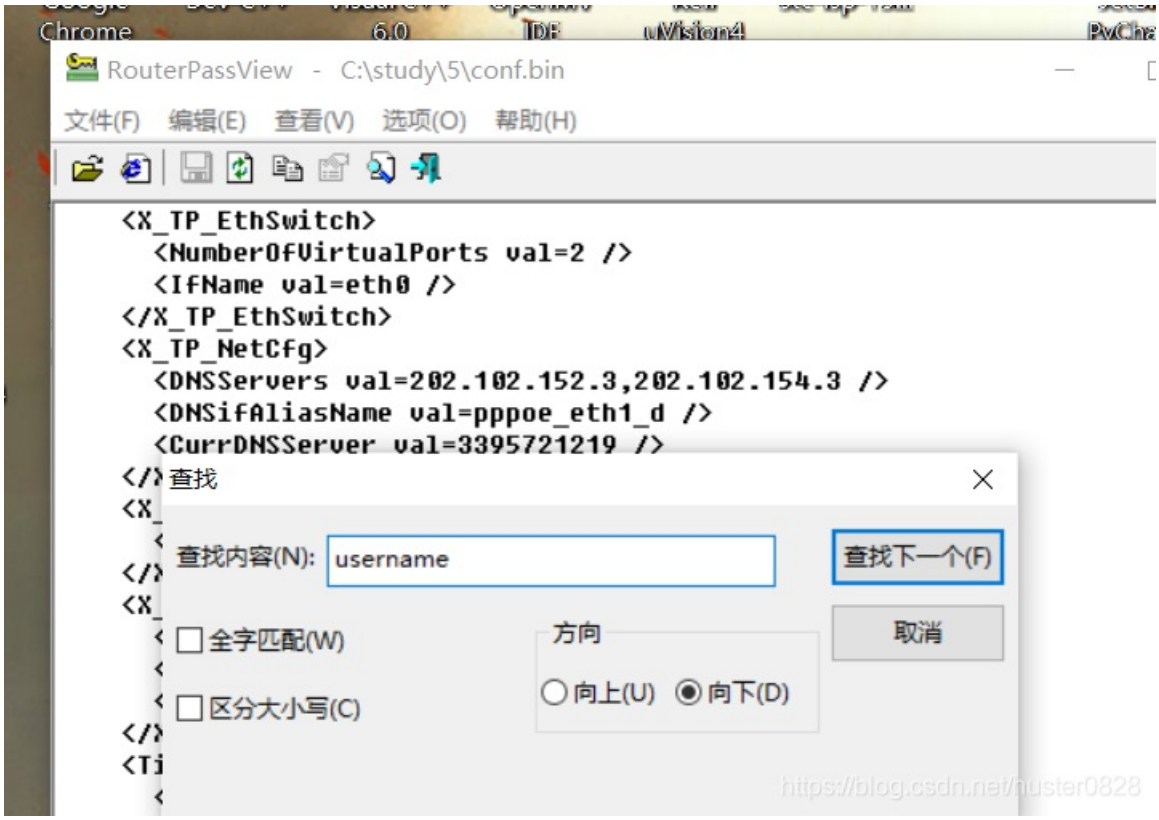
![在这里插入图片描述](https://img-blog.csdnimg.cn/20201118151516974.png#pic_center

conf.bin - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

鬻椻r1DU鲇CQ.逻烂?□ 省?衆)&/笞wL]?铘□y?j???i□(軷M?鬯陼
尅D?饯 d坎齷x}磛□oq&X記?$€
?殗1割緟?瘫 7?6??帠?蒁h盥6?圾□又p稈wa>□?杵w3濡??E%u?
□|?麭?瓣p脤?G 恳賑□慊?U梭巕P&□?怢竜?4訐L豅髦怢?□?f?刪飯
-?g?V雯鴄□u嗔o□ !?鲶QT锇3CX?鼜 衤 盹Q%"秣
i閟煁婘幱睹粲]T[6□c?t?^?u□?□?□鞢?區w?獊w? &貼?鄧忭诊
?}q撱,届xM G
Z1`遂e婷W侪S椸5)缊v澗遝?v],NJ\.□ m屡檸鶸V鰝 媽□蹀□???
n?ZaRR 婩F 蔏v?祖溦□??8?洮娘□ ?蹲?y≠?N[Z禦_ C?區wx?
□7□g>□$O1醉裉 酅4□6k发語B縚离b6(f匿钥&"d蝻□d恣遒fZ□

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



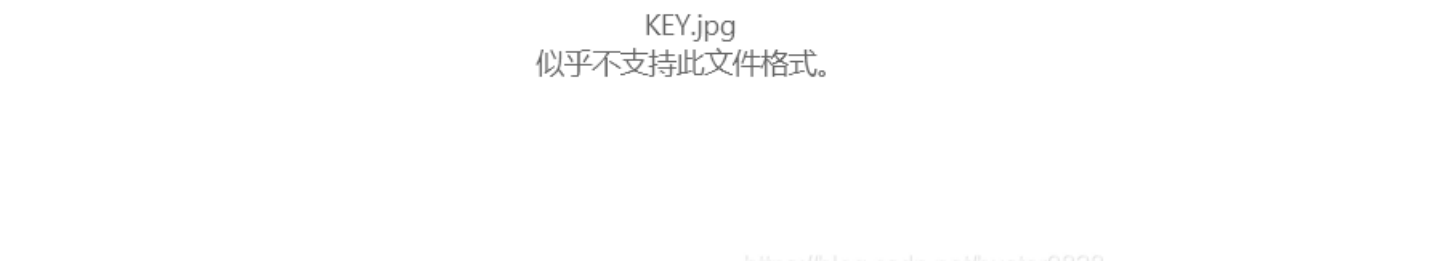
搜索用户名,然后就找到flag啦

```
<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 />
```

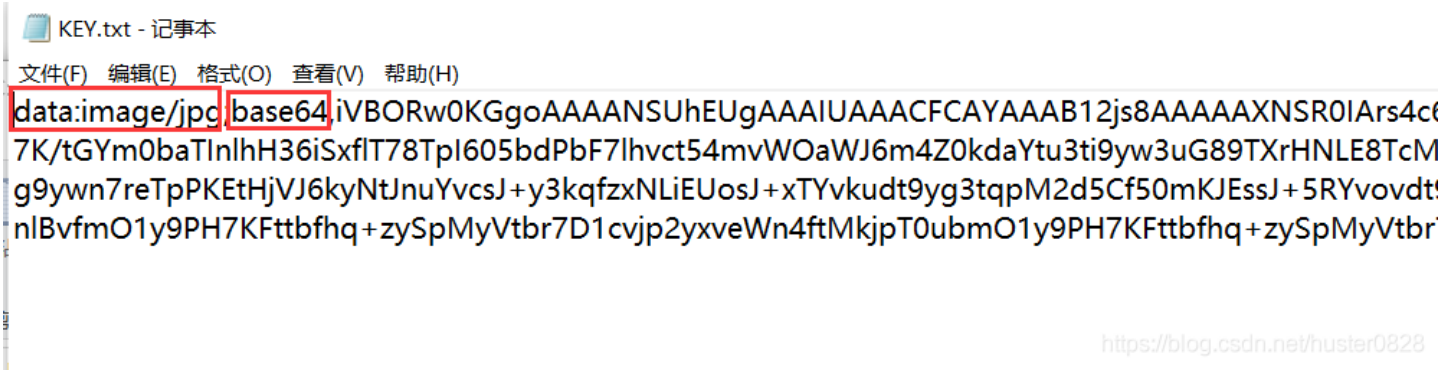
14. 多种方法解决(from Bugku)

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

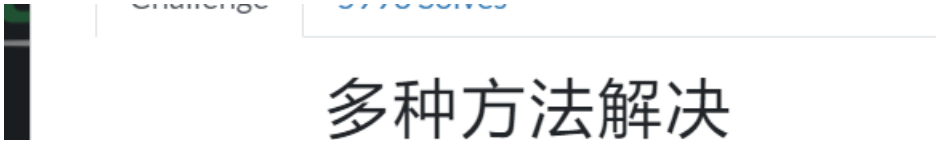
我将它改成jpg,但是打不开



然后将它改成txt,然后发现了jpg的图片和base64编码



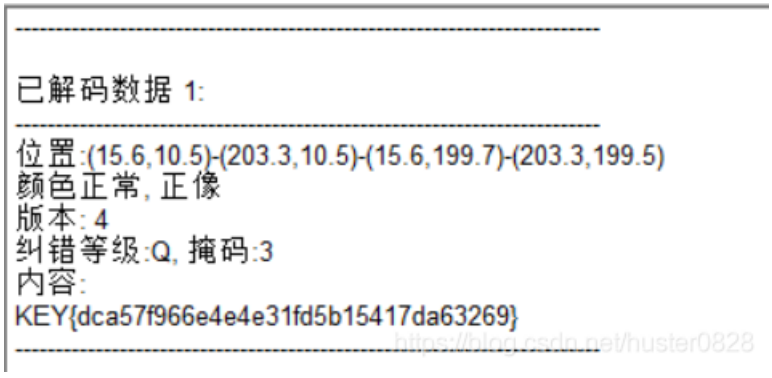
再根据题目说做题过程中会得到一个二维码



然后就找了了把banse64转换成图片的网站

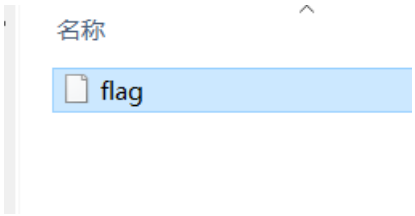
link.

再用QR识别一下二维码，就找到flag啦~



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

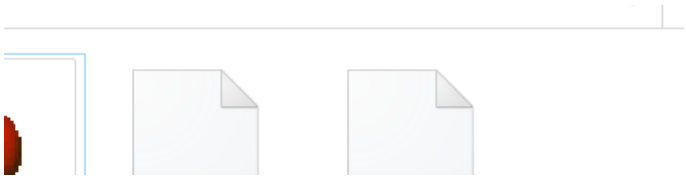
```
_娟鵑z??>g藥G0覣S??#}  ?6p%?j?C?堝鞳□?D皈吃
KEY{24f3627a86fc740a7f36ee2c7a1c124a}
```

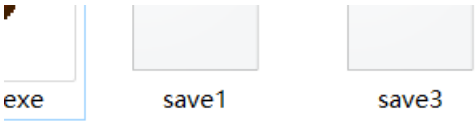
然后就找到了

17.come_game(from Bugku)

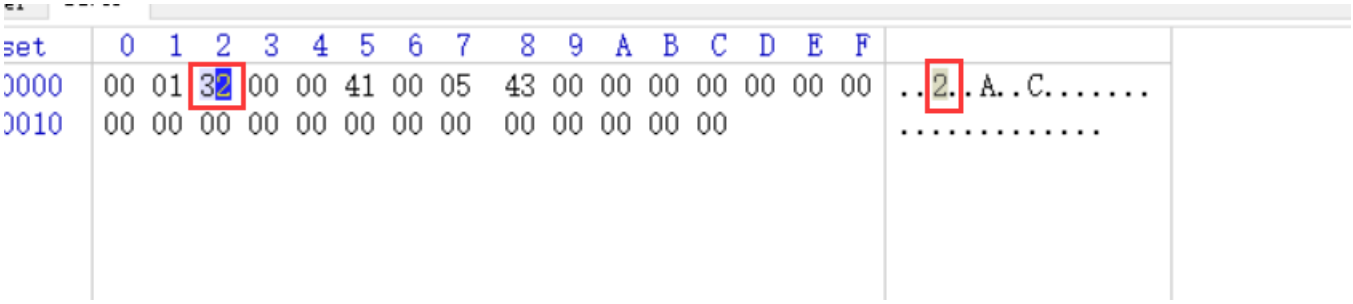
下载下来是一个文件包，解压之后有一个游戏

玩了之后发现多出了几个文件

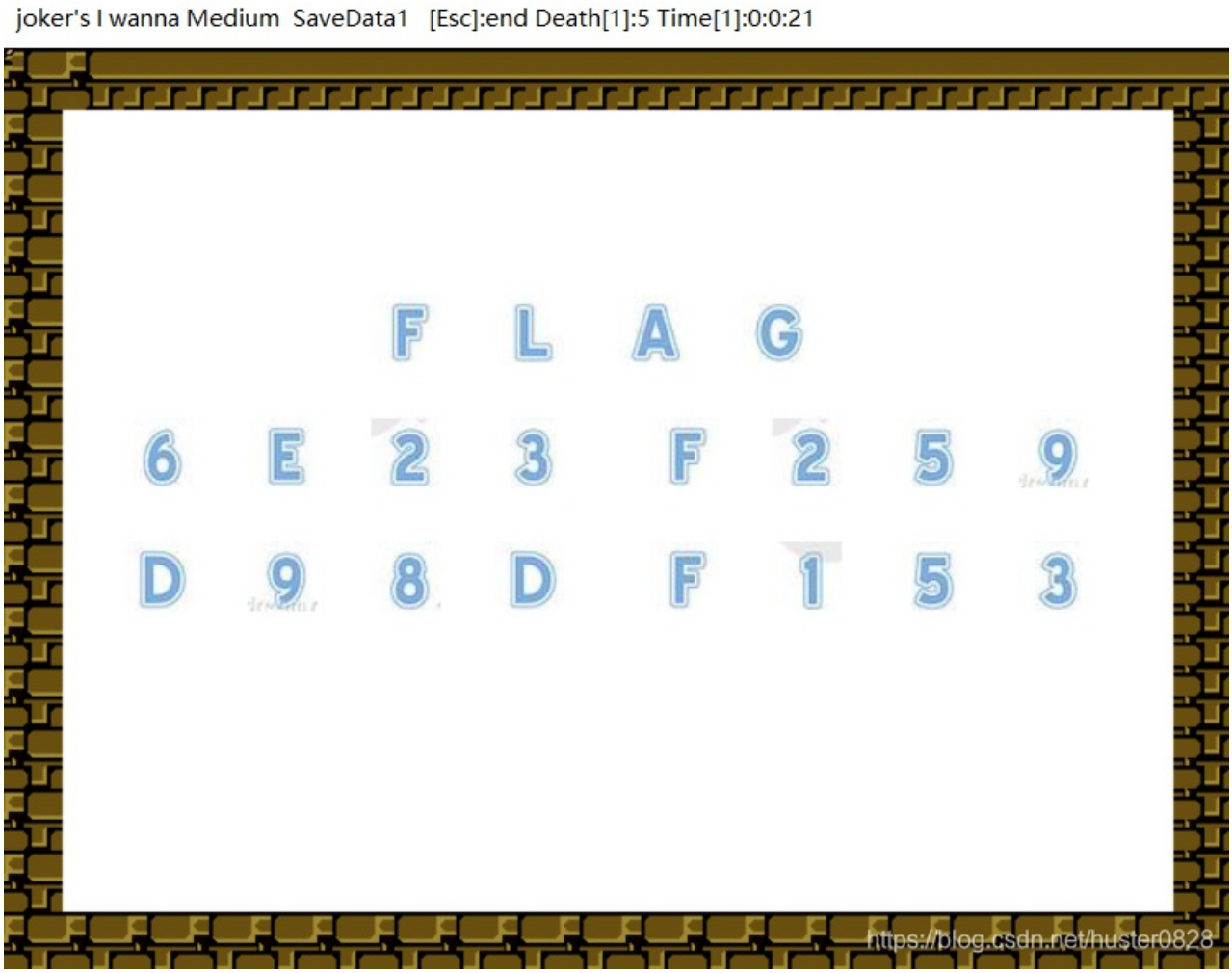




用winhex打开，发现32对应的是第二关



然后我们改成35,然后就得到flag啦

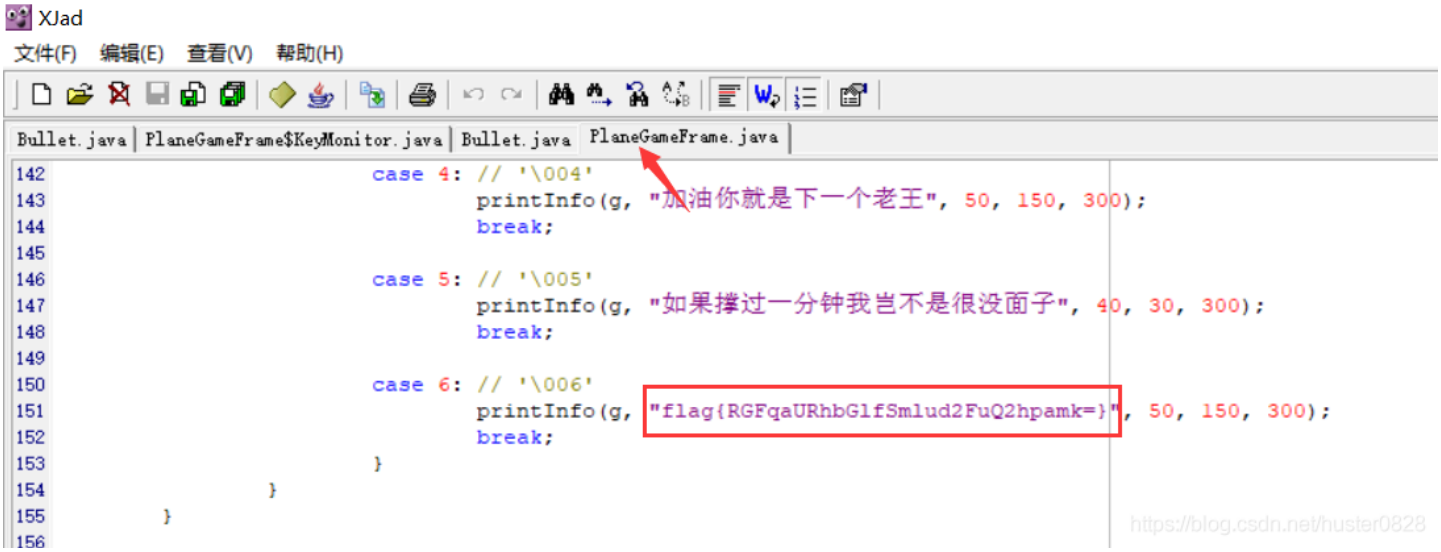


18. 做个游戏(from Bugku)

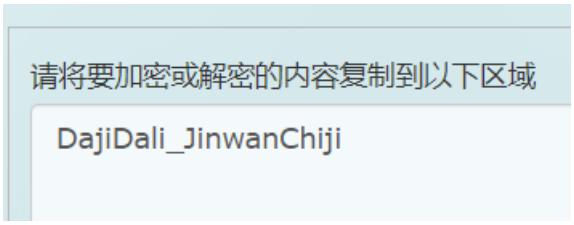
里面是一个.jar的游戏

heiheihei.jar

玩了好几次都过不了关，然后用反编译软件打开

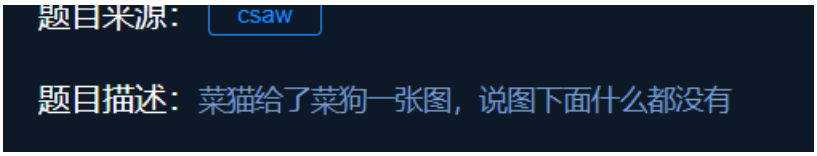


就找到flag啦，flag里面有=，应该使用base64加密



19. pdf(from 攻防世界)

打开是一个pdf，根据题目的提示



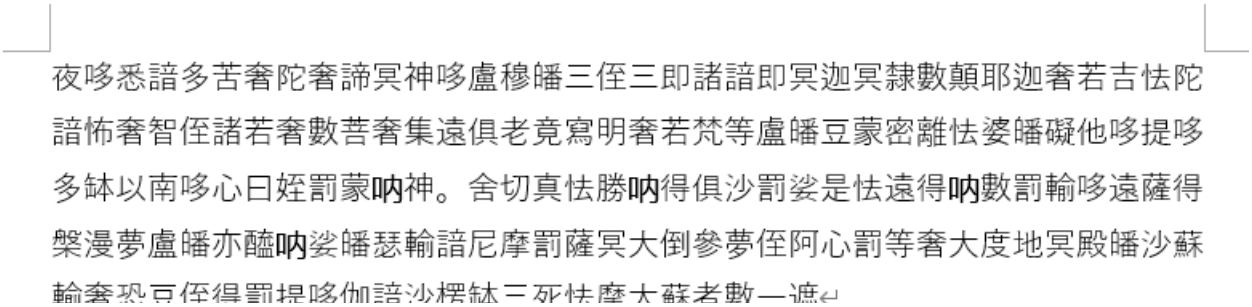
说明图片下面有东西，然后用朗读此页内容，发现里面有隐藏的东西

然后pdf转为word文档

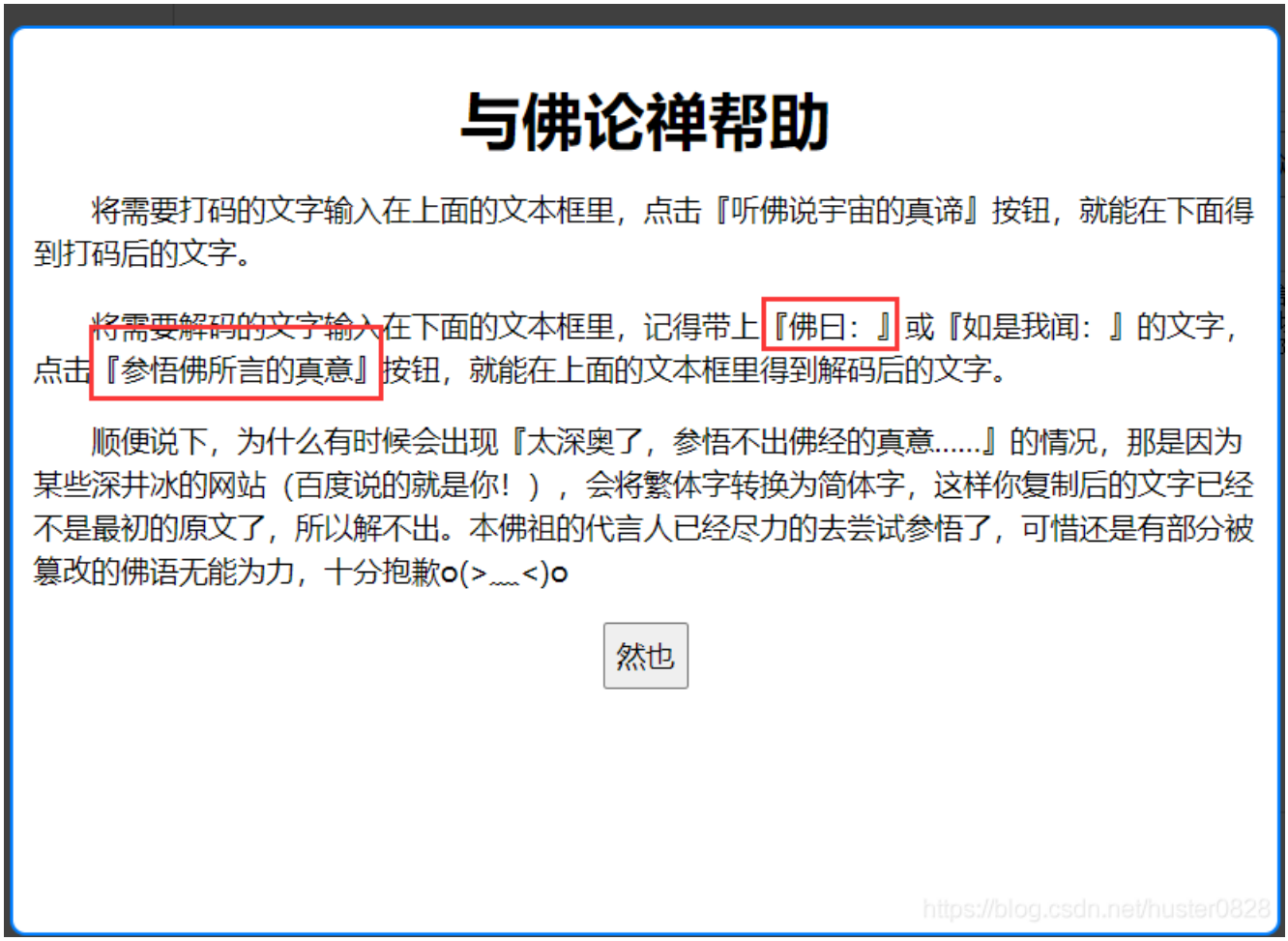
然后就找到flag啦，可以直接复制下来
flag{security_through_obscurity}

20. 如来十三掌(from 攻防世界)

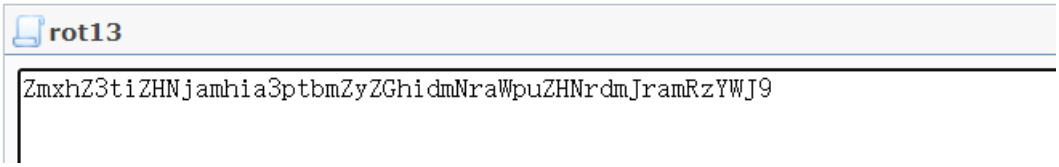
打开是一个word文档


夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多鉢以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧皤亦醯吶娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞鉢三死怯摩大蘇者數一遮

看不懂，在网上搜了一下佛语加密，就出现了在线解密工具



然后base64解密不了，再根据题目如来十三掌，猜测是ROT１３解密



再base64解密，就得到flag啦