# Mise

## this\_is\_flag

签到题flag{th1s\_!s\_a\_d4m0\_4la9}

## pdf

打开图片，flag值在图片底下，wps将pdf转为word格式后，将图片拉开发现flag



flag{security\_through\_obscurity}

## gif



刚开始给了是黑白图片，用照妖镜winhex，没发现东西，他真好给104个图片，想想正好有13个对二进制。

就写了一个脚本

> white = open("0.jpg","rb").read()

black = open("1.jpg","rb").read()

color = ""

for i in range(104):

with open("%d.jpg"%i,"rb") as f:

if f.read() == white:

color += "0"

else:

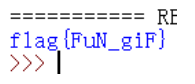
color += "1"

flag = ""

for i in range(13):

flag += chr(int(color[i\*8:(i+1)\*8],2))

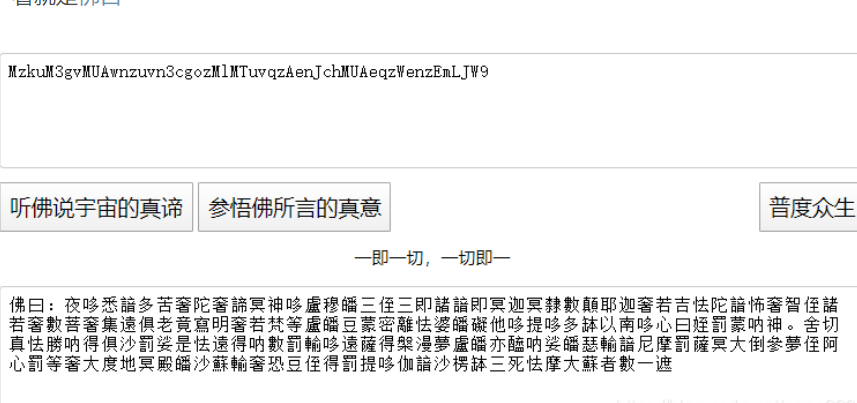
print(flag)

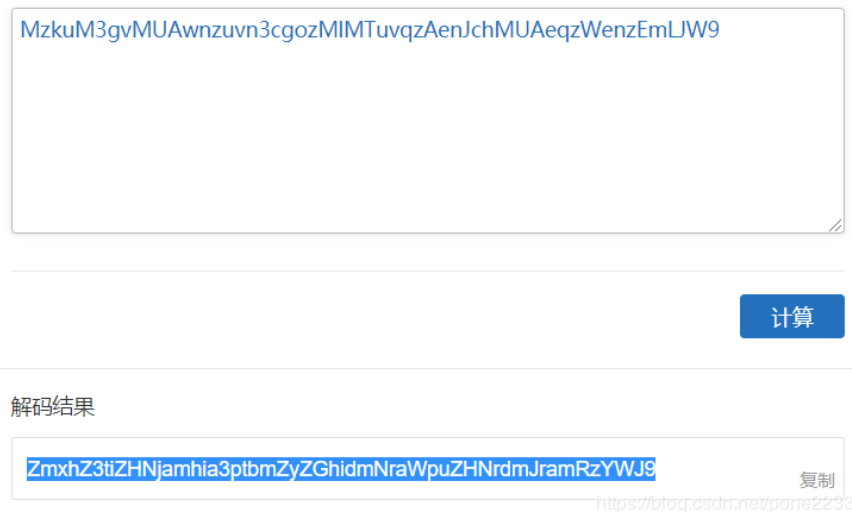


就出来了答案

flag{FuN\_giF}

## 如来十三掌

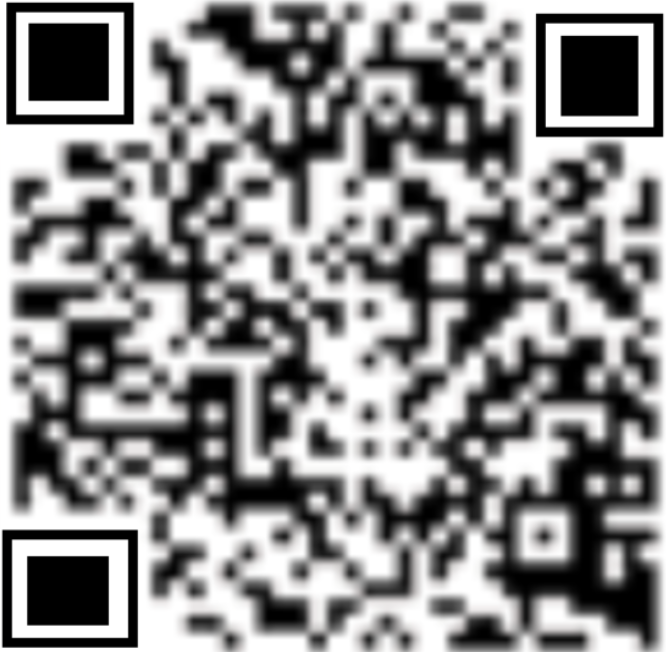
一看就是[佛曰]



这个一看就是类似于base64的加密，可惜不是，就找相似的[Rot13]最后就是[base64]

flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

give\_you\_flag

flag{e7d478cf6b915f50ab1277f78502a2c5}

坚持60s

一个做好的小软件，我们用一个很好用的反编译软件jd-gui

flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}一看就是base64

flag{DajiDali\_JinwanChiji}

掀桌子

### 发现这个应该是16进制，正好是118个，发现转换成ASCII码不行，试一下发现要-128，

### 然后就开始写一个脚本

### > import re

### a = 'c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2'

### b = re.findall(r'.{2}',a)

### flag = ''

### for i in b:

### flag += chr(int(int(i,16)-128))

### print(flag)

### 万能的py脚本

### > Hi, FreshDog! The flag is: hjzcydjzbjdcjkzkcugisdchjyjsbdfr

### > flag{hjzcydjzbjdcjkzkcugisdchjyjsbdfr}