




catf1ag Misc writeup(wp) 可能会持续更新

原创

是Mumuzi  已于 2022-02-17 21:39:38 修改  1538  收藏 3

分类专栏: [ctf](#) 文章标签: [信息安全](#) [python](#)

于 2021-12-31 19:20:43 首次发布

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_42880719/article/details/122256008

版权



[ctf](#) 专栏收录该内容

75 篇文章 28 订阅

订阅专栏

我不是很推荐连附件都不下载就直接看wp学习然后提交flag 更不推荐看都不看为了上分提交flag。

但我还是要把flag放出来(

文章目录

师傅们，看这里!!!
签到题
height
LSB
|_Love_Math
0和1
just_zip
enjoy
哇！好多文件啊
恰恰相反
BOOM!!!
加密?-M
syr2
杰瑞说我的手呢？
你以为这还是base64？
BOOM-续章
lsb看了都说big
这是谁
套神的真传
easy_base64
哪？
审查元素
这么辛苦giegie也不会心疼
random_misc
CC大学-M
这可厉害了
BOOM-2
过年了过年了
double-trouble-Hex
BOOM-3
无字天书
好像是伪加密
mzq的抄写
洁白无暇-1
拼音
2022红包题(rgba)
easy_py正则
vfree的成绩单

师傅们，看这里!!!

懒得的哥哥们，看这里!!!

```
catflag{ni79h10k5vuj8zymqxs3f4l6potarw2gcde}
```

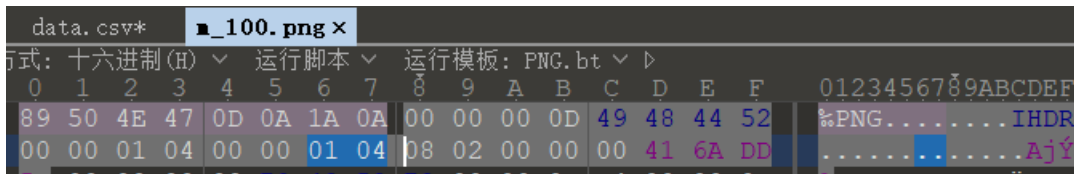
签到题

题目问建党一百周年是多久，格式为zygsctf{xxxx_xx_xx}

自己做

height

修改图片高度即可（随便拿张图举例）

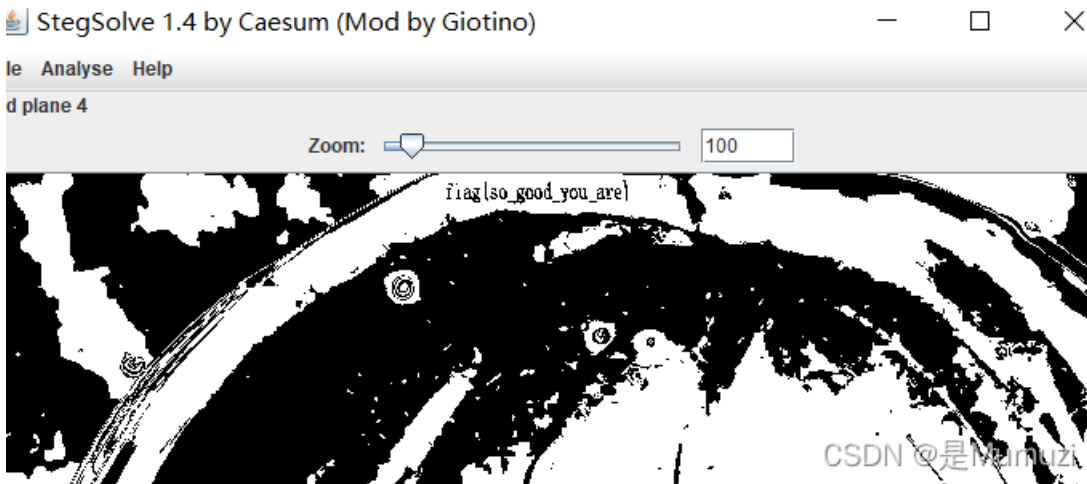


```
flag{height_and_width}
```

LSB

我不得不说 这题挺傻逼 不能大一点吗

flag在头发处



```
flag{so_good_you_are}
```

I_Love_Math

参考<https://cache.one/read/13135945>

赣网杯2021 原题

```
flag{L1n34r_R3g7e5S10n_A_G00d_Thing}
```

0和1

0转成白色 1转成黑色 画33*33的图

然后把定位点补齐扫码即可

```

from PIL import Image
f = open('01.txt', 'r').readlines()
pic = Image.new('RGB', (len(f), len(f)), (255, 255, 255))
for i in range(len(f)):
    for j in range(len(f)):
        if(f[i][j] == '1'):
            pic.putpixel((j,i), (0,0,0))
pic = pic.resize((len(f)*10, len(f)*10))
pic.save('fl111lag.png')

```



```
zygsctf{qrcode_is_fun}
```

just_zip

密码是QQ群号即226836122，解压出来的图片改zip再解压，flag在得到的图片的文件尾

```
catflag{WqPa1lob0SL8m4YsHJkNmKBYTG7jxES}
```

enjoy

PDU解码+变异凯撒

[点我解码](#)

```

s = '^m^cw\oX`[_hMPM_PUINC'
for i in range(len(s)):
    print(chr(ord(s[i]) +i+5),end='')

```

```
catflag{enjoy_catflag}
```

哇！好多文件啊

7z打开文件，发现4.txt的CRC与其他的不同，于是打开4.txt，搜索zygs即可

```
zygsctf{p8071txoqh4m3rj9wysk5defgzuv62}
```

恰恰相反

盲文密码，得到的flagreverse即可，然后dala改成dalao
参考<https://www.cnblogs.com/liume/p/10104530.html>

```
catflag{dalao666}
```

BOOM!!!

伍，5个数字，AAPR爆破得到密码57632，解压即可

```
zygsctf{r36178w9vgtmp5jhzusbi0dokayqlxef2c4n}
```

加密?-M

扫码，蓝奏云下载附件，得到的txt附件是0宽字符隐写，解出来得到长度115(5的倍数)的01字符串，培根密码解密即可
注意是小写

```
flag{dalaodaidaiwowuwuwu}
```

syr2

很明显的看出，png的字节倒了过来，于是写个脚本再reverse一下

```
f = open('flag1.png', 'wb').write(open('flag_syr2.syr2', 'rb').read()[::-1])
```

得到二维码图片，扫码

得到@iH<,{FT7RYs<P{iWP0=<[A+EW

base91解码得到flag

```
flag{ccd_x_hacker_tq1}
```

杰瑞说我的手呢？

png图片

```

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
32 33 33 33 00 00 00 0D 49 48 44 52 00 00 00 ED 2333....IHDR...í
00 00 00 F1 08 02 00 00 00 A8 3B A7 38 00 00 20 ...ñ.....";$8..
00 45 41 53 59 78 01 EC DD 5B B3 24 49 72 18 E6 .EASYx.ìÝ[³$Ir.æ
BA 57 9D 7B 77 CF CC 2E B1 00 49 01 90 28 52 32 °W {wİİ ± I (B2

```

改成

```

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
: 00 00 00 ED 00 00 00 F1 08 02 00 00 00 A8 3B A7 ...í...ñ.....";$
: 38 00 00 20 00 45 41 53 59 78 01 EC DD 5B B3 24 8.. .EASYx.ìÝ[³$
: 49 72 18 E6 BA 57 9D 7B 77 CF CC 2E B1 00 49 01 Ir.æ°W {wİİ ± I.

```

此时图片还是出错

上图能注意到，IDAT的位置被改成了EASY

于是将EASY改成IDAT

```

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
00 00 00 ED 00 00 00 F1 08 02 00 00 00 A8 3B A7 ...í...ñ.....";$
38 00 00 20 00 49 44 41 54 78 01 EC DD 5B B3 24 8.. .IDATx.ìÝ[³$
49 72 18 E6 BA 57 9D 7B 77 CF CC 2E B1 00 49 01 Ir.æ°W {wİİ ± I.

```

即可得到flag

```
flag{QLNU666666}
```

你以为这还是base64?

在文本前面加上data:image/png;base64,

然后浏览器打开即可

```
zygsctf{ziyougongshi}
```

BOOM-续章

jpg的属性发现cGFzc3dvcmQ6dmZyMTE=, 解码得到密码vfr11

当然爆破也行

flag改成flag.zip

```
zygsctf{yxgm3cukn0vhqtdji5ez7r8bw1269aops4f1}
```

lsb看了都说big

见<https://blog.csdn.net/zip471642048/article/details/121734206>

这是谁

见<https://blog.csdn.net/zip471642048/article/details/122018742>

套神的真传

见<https://blog.csdn.net/zip471642048/article/details/122018326>

easy_base64

为什么不手撸而要写脚本呢
是手撸不快了吗

```
zygsctf{4j2ag83qxdhuwoyr76c91szv01ekb5mtifpn}
```

哪?

百度识图，西安钟楼

```
zygsctf{xi_an_zhong_lou}
```

审查元素

公告栏!!!公告栏!!!那里F12能看到
class="No Hs Bk Lr Db Uup Lr Rg Rg Fm"
原子序数转ascii字符即可

```
s = '102 108 97 103 105 115 103 111 111 100'  
s = s.split(' ')  
for i in s:  
    print(chr(int(i)),end='')
```

```
zygsctf{flagisgood}
```

这么辛苦giegie也不会心疼

问flag在哪 答叫输入whereis flag
问whereis flag 答flag in /etc/f1ag
问tac /etc/f1ag
答

```
catflag{hxfumesglji7o2n0pdk1y8w5r3tv9baz6c4q}
```

random_misc

首先猜测格式 flag、catflag、zygsctf
进行爆破，找出e的值
测试之后发现能得到200 182 93 227 25 182 236的是catflag
顺便就得到了e的值28560，除以255即112。如下

```
from random import randint  
from math import floor, sqrt  
a = ''  
b = 'catflag'  
d = [ ord(c) for c in b ]  
for e in range(65,127):  
    e = e * 255  
    for c in range(len(b)):  
        a += str(int(floor(float(e + d[c]) / 2 + sqrt(e * d[c])) % 255)) + ' '  
    print(a)  
    a = ''  
    print(e)
```

然后爆破即可，如下

```
from random import randint
from math import floor, sqrt
a = ''
e = 112 * 255
b = "200 182 93 227 25 182 236 150 60 245 254 84 164 254 84 164 227 101 42 42 134 222 166"
b = b.split(' ')
for c in range(len(b)):
    for i in range(32,128):
        tmp = str(int(floor(float(e + i) / 2 + sqrt(e * i)) % 255))
        if(tmp == b[c]):
            a += chr(i)
            break
print(a)
```

得到flag:catfla5{This_is_funny!}

然后5改成g即可

```
catflag{This_is_funny!}
```

CC大学-M

属性里面有一句话

md5(CCDX_CTF)

文件尾有一个zip文件，手动分离一下

然后这里的md5是16位的这里加密

得到密码464d81f01c215e93

即可成功解压zip文件

```
flag{ccdxcctf-ce78d1da254c0843eb23951ae077ff5f}
```

这可莉害了

压缩包最下面“出去玩”对应out

猜测outguess

可莉双倍快乐，可莉生日0727

双倍即07270727

使用outguess

outguess -k "07270727" -r file.jpg Klee.txt

得到密码

```
klee~klee~klee
```


得到第二张图片

第二张图片文件尾是一个base64串，不能直接解，猜测对称加密。

没想到的是直接在这里搜klee就能找到key了

```
.h@.,°xÁß5†o.klee  
e's treasure:.be  
ng_beng_zha_dan!  
&vcbAA(Tnu,-Ã*
```

AES加密模式: 填充: 数据块: 密码: 偏

待加密、解密的文本:

```
o+nzZSjmLVQS6C5a3BB1NbjefbkLiGj8sfGDSWGXT0YCb1eA8ao6lWwsEbmPdMkK
```

↑ 将你电脑文件直接拖入试试^-^

AES加密

AES加密、解密转换结果(base64了):

```
catflag{klee_want_to_play_with_you!}
```

CSDN @是Mumuzi

```
catflag{klee_want_to_play_with_you!}
```

BOOM-2

使用rockyou字典爆破，得到密码

解压出来的密文尝试凯撒并不正确，于是猜测维吉尼亚

反向测试发现key为mz

得到flag

```
catflag{508855ee-6ac1-11ec-97ae-3c7c3fb9e9bb}
```

过年了过年了

-的意思是负 而不是分隔符

题目第一反应是日历和数字有关然后猪圈密码，但是最后发现6位一组的话，且大小都是在19w~25w内活动，猜测是要除以一个数字。且对200277、196037进行分解之后，明显发现196037分解之后是2021*97

根据过年了，于是猜测是都除以一个2021，且200277//2021=c，符合catflag的开头

脚本如下

```
s = '200277-196037234668-206142218484-196037208369-248583139587-238478224553-218268236691-234436212415-224331222  
530-196037230622-244541192185-238478196231-230394212415-196037234668-212205224553-222310192185-224331206346-1919  
95135541-196037204323-232415196231-230394252875'  
s = s.split('-')  
print(chr(int(s[0])//2021),end="")  
for i in range(1,len(s)):  
    for j in range(2):  
        print(chr(int(s[i][6*j:6*j+6])//2021),end='')
```

```
catflag{Evolutionary_variation_of_Caesar}
```

double-trouble-Hex

第一步是twin-hex，找到在线网站解码即可。

<https://www.calresult.com/misc/cyphers/twin-hex.html>

第二步是爆破emoji-aes，把源码下载下来找到对应关系，然后爆破aes,aes-base64他用的是crypto-js，总之写个脚本爆破就行了。

但是好像也能直接调用来进行爆破(?)

我不会 我写的脚本，总之爆破得到flag和key

```
catflag{twin-hex_and_emoji-aes}
```

BOOM-3

百度找个脚本爆破就行了，然后搜索flag

```

def decrypt():
    k1 = [1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25]
    n = 1
    ny = []
    for i in k1:
        while (i * n) % 26 != 1:
            n += 1
        ny.append(n)

    w = open('plain08.txt', 'w')
    cipher = 'cqznjpszccjmrvjyirekxxbkxxb'
    p = []
    for k1 in ny:
        for k2 in range(1, 27):
            p.append('\n 逆元=' + str(k1) + '    k2=' + str(k2) + '    ')
            # plain = ''.join('\n 逆元='+str(k1)+'k2='+str(k2)+'    ')
        for i in range(len(cipher)):
            # 小写字母
            if cipher[i].islower():
                t1 = ord(cipher[i]) - 97 - k2
                if t1 < 0:
                    t1 += 26
                p.append(chr((k1 * t1) % 26 + 97))
            # 大写字母
            elif cipher[i].isupper():
                t2 = ord(cipher[i]) - 65 - k2
                if t2 < 0:
                    t2 += 26
                p.append(chr((k1 * t2) % 26 + 65))
            # 其他
            else:
                p.append(cipher[i])

        plain = ''.join(p)
    w.write(plain)
    print('解密完成! ')
    w.close()

if __name__ == '__main__':
    decrypt()

```

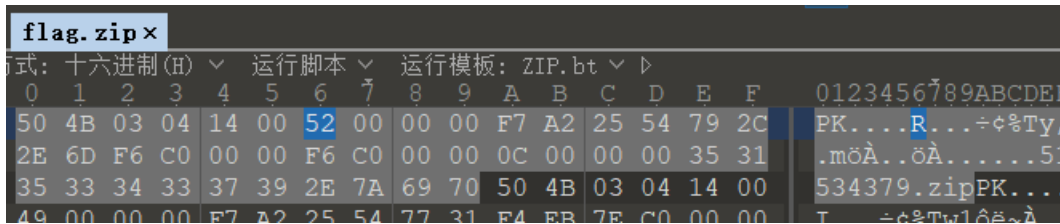
```
catflag{flagisaffinecipherboomboom}
```

其实我刚开始是想直接梭quipqiup
 但是最后差最后8个字母没猜出来是boom
 可以看看我的想法，没啥实际用处：首先quipqiup猜测密文对应关系
 cqznpjzccjmrviyrekxxbkxxb
 flagis
 然后发现c此时对应上了f，cc正好对应上了affine
 然后发现
 cqznpjzccjmrviyrekxxbkxxb
 flagisaffine
 此时又发现j对应上了i正好仿射密码完整的是affine cipher
 直接就猜到对应关系是
 cqznpjzccjmrviyrekxxbkxxb
 flagisaffinecipher
 最后就差kxxbkxxb，emm，没猜出来，结果还是去找脚本了属于是。

无字天书

长安“战疫”网络安全卫士守护赛的题，直接交了
 flag和wp详细看另一篇博客

好像是伪加密



这里，写个脚本每次都提取出

来，并且改成00来循环解压

```
import zipfile
import os
s = ''
name = 'flag'
try:
    while True:
        f = open(f'{name}.zip', 'rb').read()
        s += str(hex(f[6]))[2:].zfill(2)
        new_zip = open('newzip.zip', 'wb').write(f[:6]+f[5:6]+f[7:])
        zipf = zipfile.ZipFile('newzip.zip')
        zipf.extractall()
        zipf.close()
        os.remove(f'{name}.zip')
        name = zipf.namelist()[0][:-4]
        os.remove('newzip.zip')
except:
    print(s)
```

解压出来的flag.txt能得到第二部分，然后上面输出的s从hex到ascii之后能得到webp文件，是一个二维码，扫码即可得到第一部分flag

```
catflag{good_job_and_zip_crypto}
```

mzq的抄写


```

from PIL import Image
n = 37
pic = Image.new('RGB', (n,n), (255,255,255))
f = open('ah.txt', 'r').read()[:66564]
for i in range(n):
    for j in range(n):
        if(f[i*n+j] == '1'):
            pic.putpixel((j,i), (0,0,0))
pic.show()
pic.save('what.png')

```



扫码得到flag

```
catflag{114514_mumuzi}
```

洁白无暇-1

文件尾有段flag密文，凯撒偏移2得到catflag(flag_is_not_here_but_in_the_a_and_b)，是fake flag

然后用stegsolve打开，稍微看一下通道能看见二维码

扫码得到catflag(flag_in_mzq_heart)，尝试提交发现是又是fake flag

再继续看通道，发现alpha通道和blue通道都有一条线在变化，用计算机自带的画图工具查看之后得到这条线是在宽为20地方
结合第一个fake flag，推测a->alpha,b->blue

于是写个脚本分别提取这条线的值

```

from PIL import Image
pic = Image.open('png.png')
h = pic.size[1]
flag = [0]*h
for i in range(h):
    tmp = list(pic.getpixel((20,i)))[2]
    if(tmp != 0):
        flag[i] = tmp
    tmp = list(pic.getpixel((20,i)))[3]
    if(tmp != 0):
        flag[i] = tmp
print(''.join(chr(i) for i in flag))

```

得到flag

```
catflag{flag_is_RGBA_secret}
```

拼音

就单纯的取拼音的声母

陈啊跳分1啊高{啊不陈的额分高好i健看了吗年哦盘群人是跳uv我小有在}

```
catflag{abcdefghijklmnopqrstuvwxy}
```

2022红包题(rgba)

010打开，发现文件尾还有一个png图片，只是PNG的头改成了MZQ，改回来然后分离出来就可以了。

然后发现分离出来的图片，每一横排的值都是一样的，猜想是竖着看。写个脚本提取一下第一列的RGBA值，发现都在可打印ascii的范围内，于是写个脚本。

```
from PIL import Image
pic = Image.open('tiger.png')
h = pic.size[1]
for i in range(h):
    s = list(pic.getpixel((0,i)))
    print(''.join(chr(k) for k in s),end='')
```

Happy new year. I wish you good health and academic success. You can bypass everything, solve all problems, and give you flag:
catf1ag{98405cc5-8288-11ec-a207-3c7c3fb9e9bb}

得到flag:

```
catf1ag{98405cc5-8288-11ec-a207-3c7c3fb9e9bb}
```

easy_py正则

只要满足 `^[c]atf[0-1]agi[s]{2}og[o]{2}d,[I]like[c]atf[0-1]ag[6]{3}$` 就可以了

[点我看看](#)

点上面的看看就知道了

所以得到vfree_doll想要的flag:

```
catf1agissogood,Ilikecatf1ag666
```

vfree的成绩单

第一部分是成绩单上的数字

From Decimal ⊗ ||

Delimiter: Space Support signed values

99 97 116 102 49 97 103 123 50 52 53 51

Output: catf1ag{2453}

CSDN @是Mumuzi

第二部分是text块的AES，密码是vfree，说实话我没找到密码在哪，这题一直卡这里了最后尝试猜密码猜到的。

U2FsdGVkX18yNX2nppxF2v0OBXU1JGisr70kGrSAn6U=

AES DES RC4 Rabbit TripleDes

vfree

加密

解密

清空输入框

复制结果文本

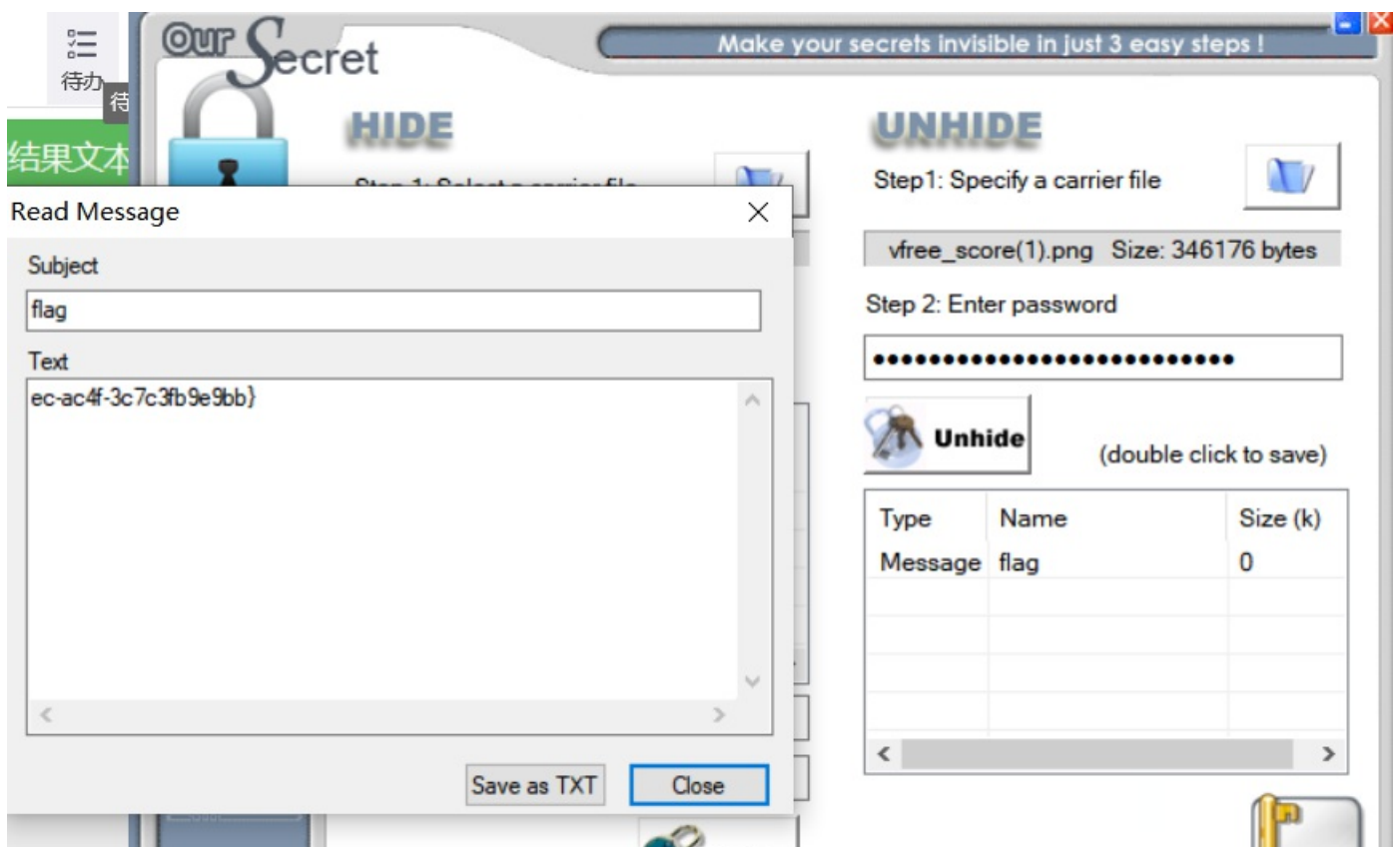
ea79-8bc7-11

CSDN @是Mumuzi

第三部分是文件尾的特征块，很明显的oursecret

```
.H@.HI..À...9l>0  
m;0>:>?ln;<0.™..
```

password在第二个text块(hongkongdoll_is_vfree_like)，当然这个password也提示了OS（oursecret）



Hide



提示了OS (oursecret)

CSDN @是Mumuzi

```
catflag{2453ea79-8bc7-11ec-ac4f-3c7c3fb9e9bb}
```