2021安洵杯Misc writeup

原创

是Mumuzi 于 2021-11-28 14:42:34 发布 740 收藏 1

分类专栏： ctf 文章标签： 信息安全 网络安全

忘了发了，来迟了

顺便发一下战队的全wp：

https://wp.n03tack.top/posts/4906/

Misc

应该算是签到

来得早不如来的巧

CyzCC_loves_LOL

小脑洞+老考点，理解一下

```
HAI D0g3 code
I HAS A CODE ITZ "D0g3isthepAssword"
I HAS A MSG ITZ ""
I HAS A COUNTER ITZ 0
I HAS A NUM
IM IN YR LOOP UPPIN YR COUNTER WILE COUNTER SMALLR THAN LEN OF CODE
I HAS A C ITZ CODE!COUNTER
NUM R ORD OF C
NUM R SUM OF NUM AN -3
IZ NUM SMALLR THAN 65?, NUM R SUM OF NUM AN 26, KTHX
NUM R CHR OF NUM
MSG R SMOOSH MSG AN NUM
IM OUTTA YR LOOP
VISIBLE MSG
KTHXBYE
```

原字符串
msg =''

循环，后面loop跳出循环
原字符串一个个ord
减3
根据问号得出判断是否小于65，小于就+26
chr到msg里

输出msg

其实是放进百度翻译然后一下看出来了

```
s = 'D0g3isthepAssword'
flag = ''
for i in range(len(s)):
    tmp = ord(s[i])-3
    if(tmp<65):
        flag += chr(tmp+26)
    else:
        flag += chr(tmp)
print(flag)
```

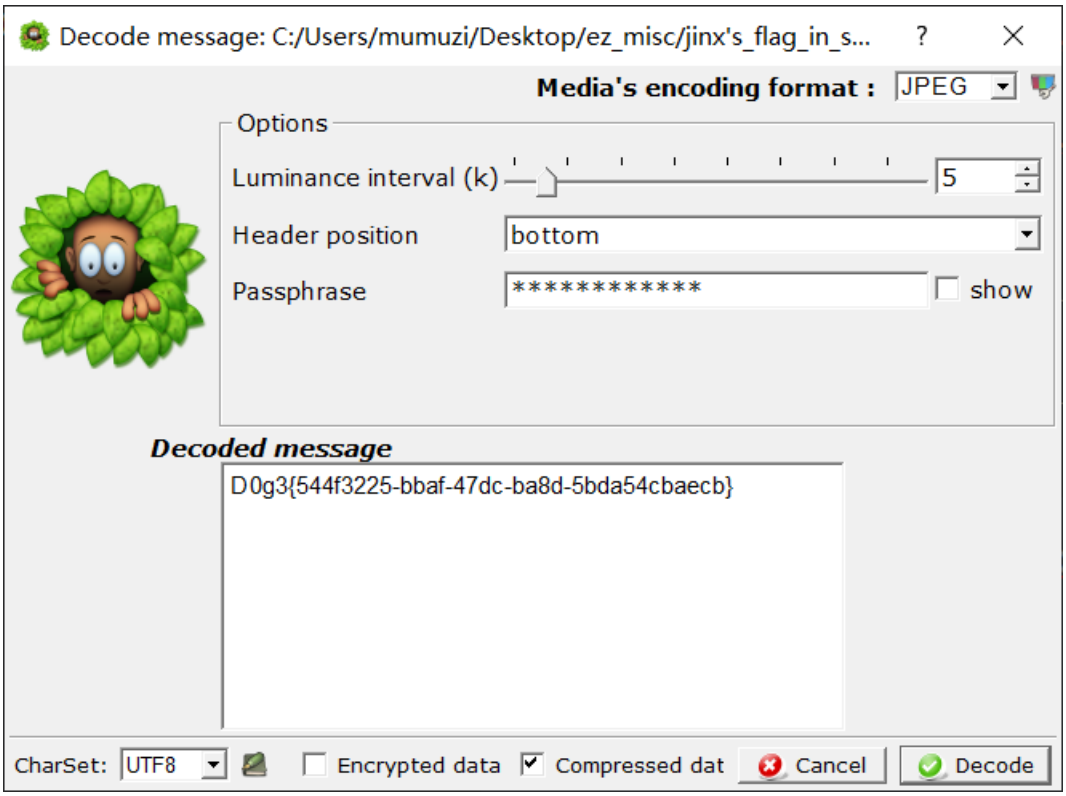
密码为AGdJfpqebmXpptloa

然后解压得到图片和图片（

jpg那个图说是silent，于是知道是silenteye，右边的图不是piet就是brainloller，试了之后发现是brainloller

然后.\bftools.exe decode brainloller .\Program.png，得到的brainfuck解码一下得到0MTTW CWZVN!，空格替换下划线即可

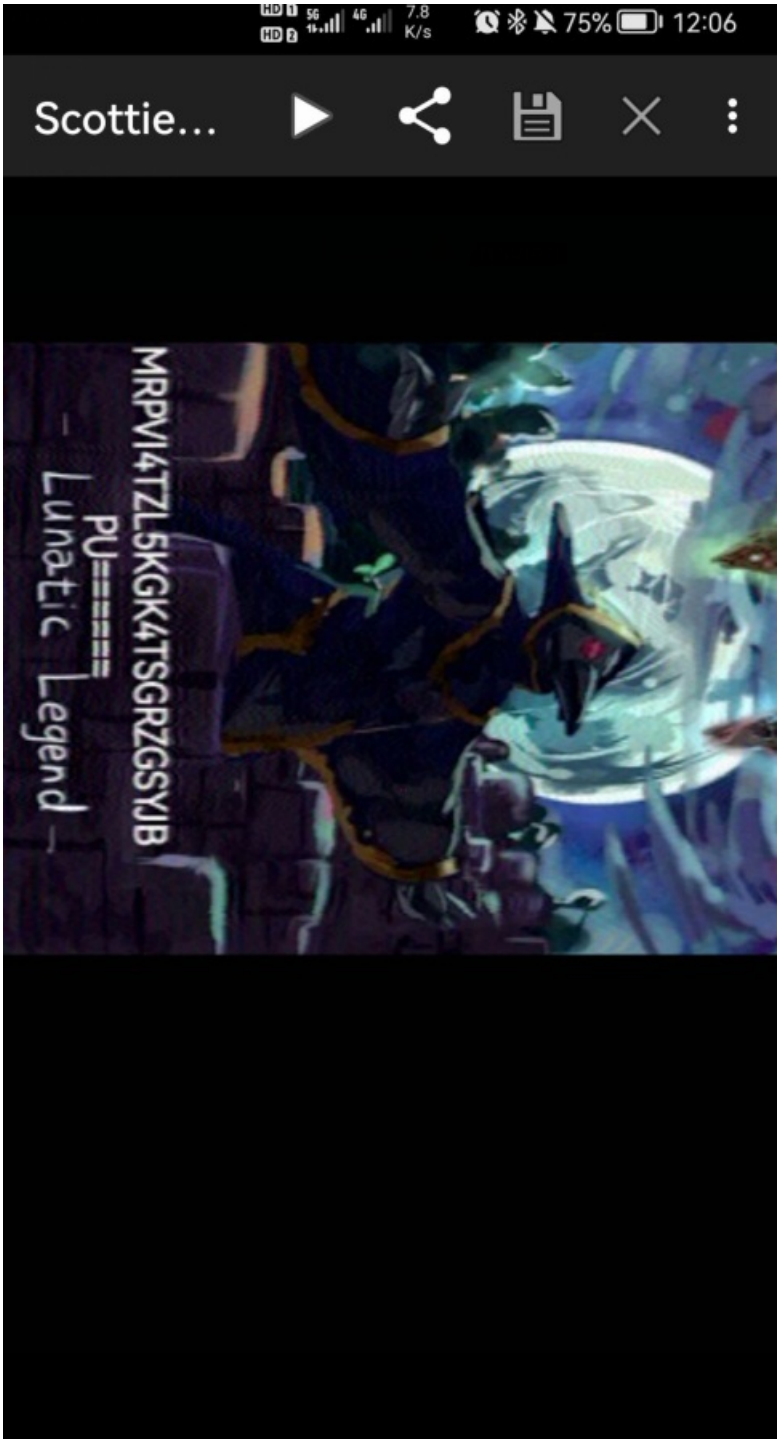
然后silenteye解jpg，密码为0MTTW_CWZVN!




```
D0g3{544f3225-bbaf-47dc-ba8d-5bda54cbaecb}
```

Cthulhu Mythos

hint.mp3是sstv，后面那段扫一下即可



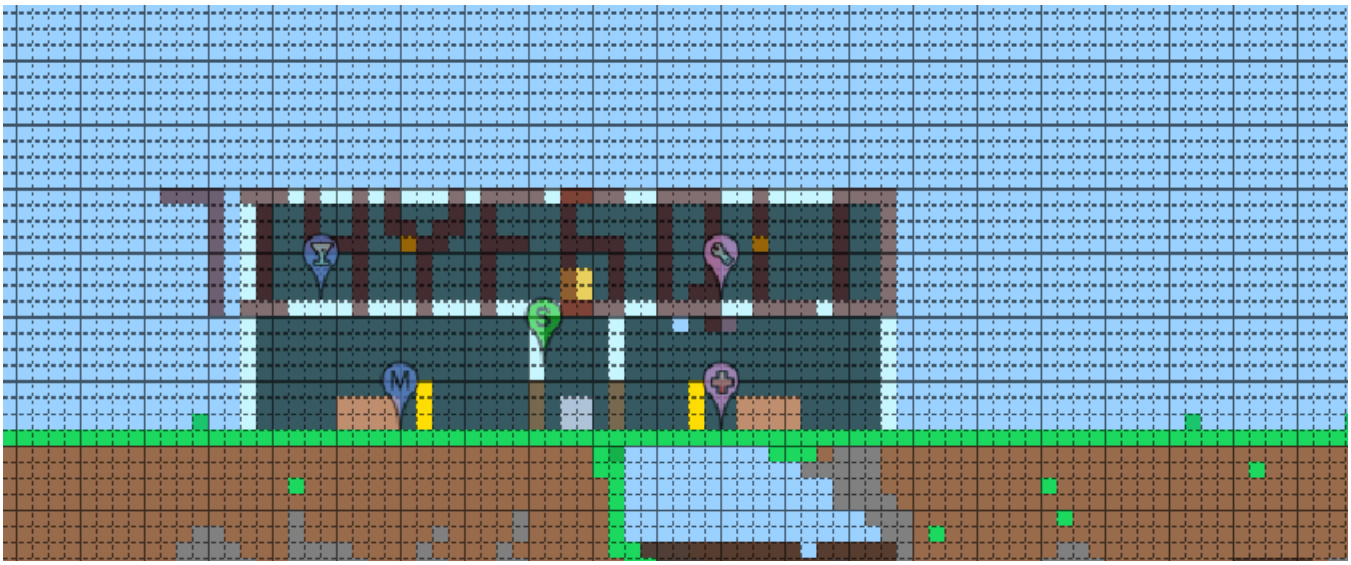
解码

```
MRPVI4TZL5KGK4TSGRZGSYJBPU======
```

Output

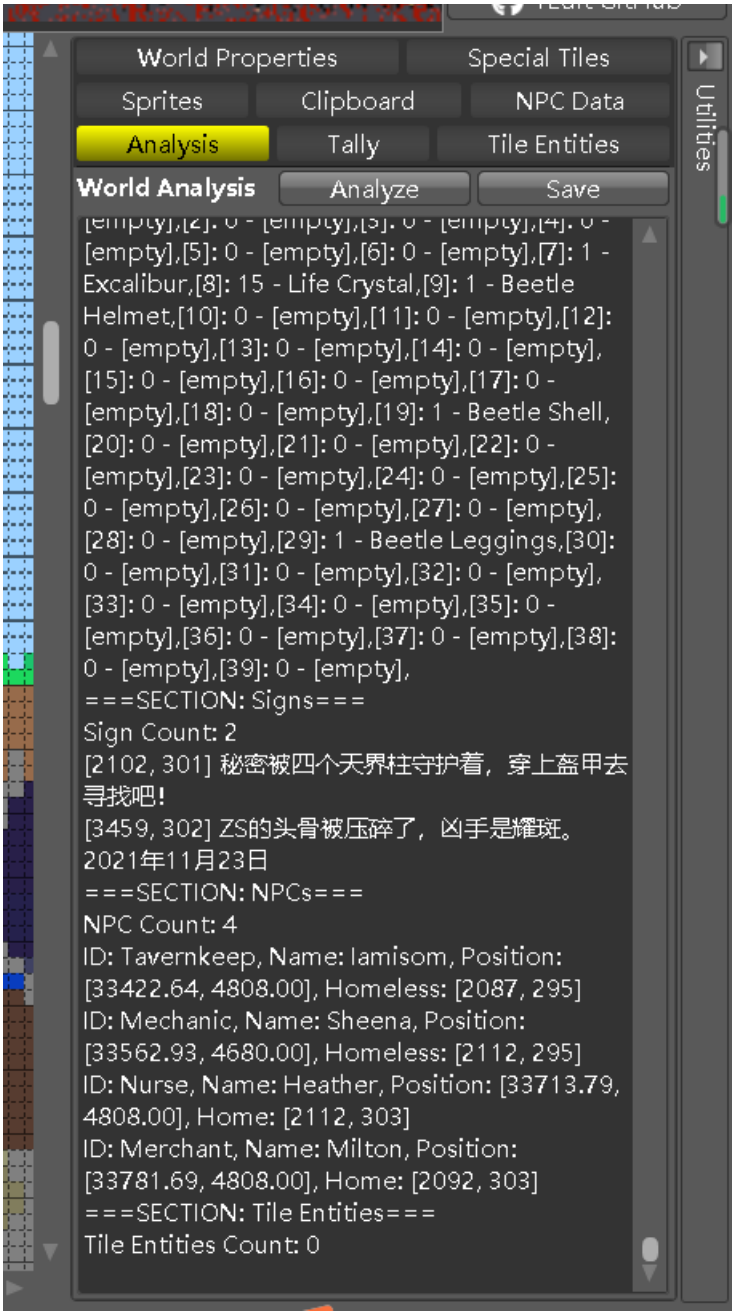
```
d_Try_Terr4ria!}
```

根据提示猜测是泰拉瑞亚，去github下载一个地图编辑器

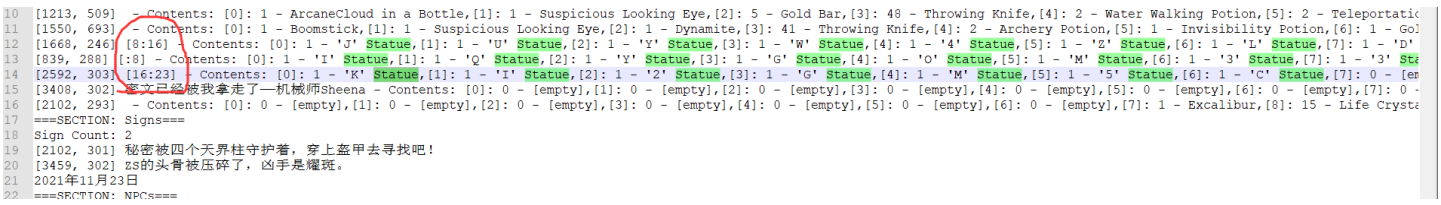


进去就看到7I4YF6QL0

然后猜测剩下的在对话里之类的，之后在分析里找到内容



导出后看txt



按顺序撸下来,得到

```
YQIGOM33JUYW4ZLDKI2GM5C7I4YF6QL0
```

Output

```
Ä.g3{M1necR4ft_G0_A`
```

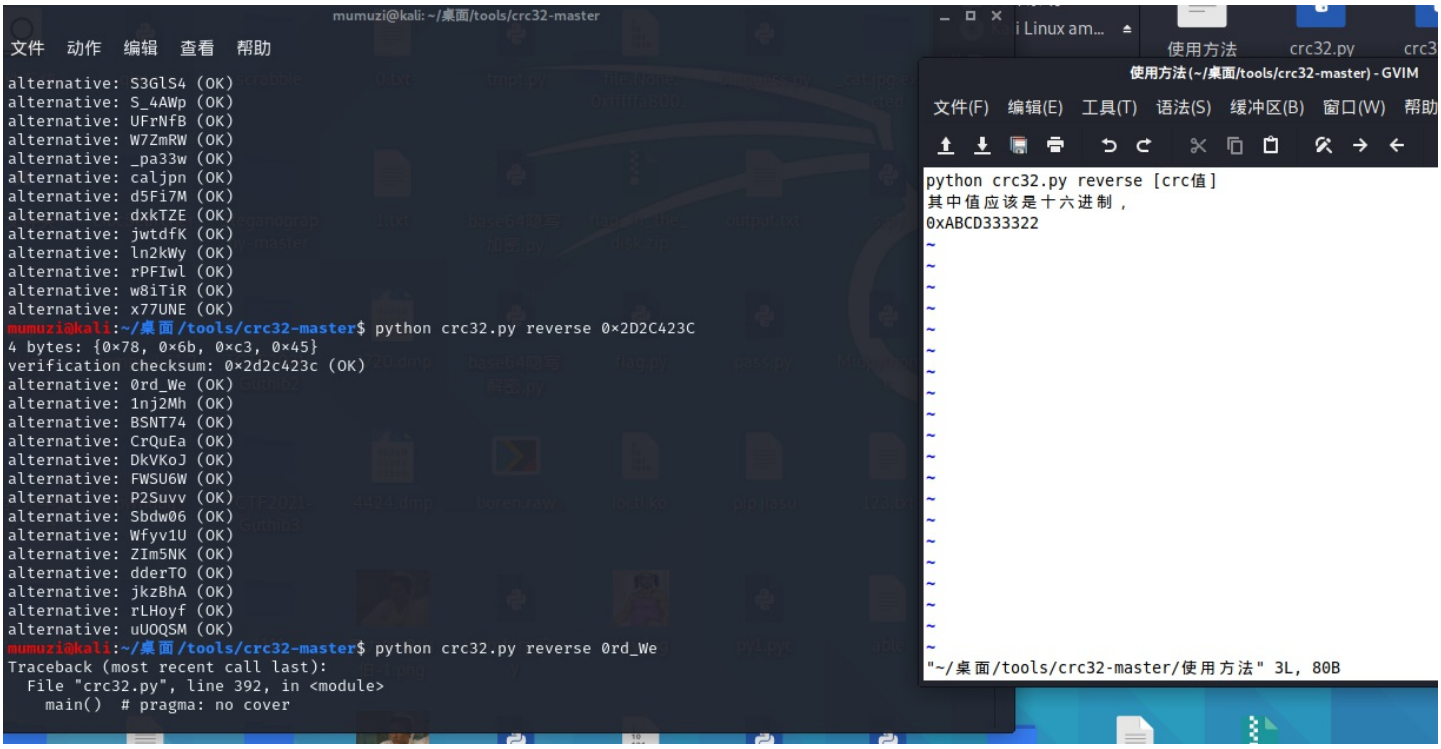
emm能看出来前面和后面都有错误，但是前面能知道是D0g3{M1necR4ft_G0_A 后面是d_Try_Terr4ria!}

然后觉得中间填and，尝试提交发现正确，所以flag为

```
D0g3{M1necR4ft_G0_And_Try_Terr4ria!}
```

lovemath

爆CRC



得到密码

th1s_ls_Y0ur_pa33w0rd_We1c0m3e

blind是LSB，BGR的，提取出来一个图片纯数字

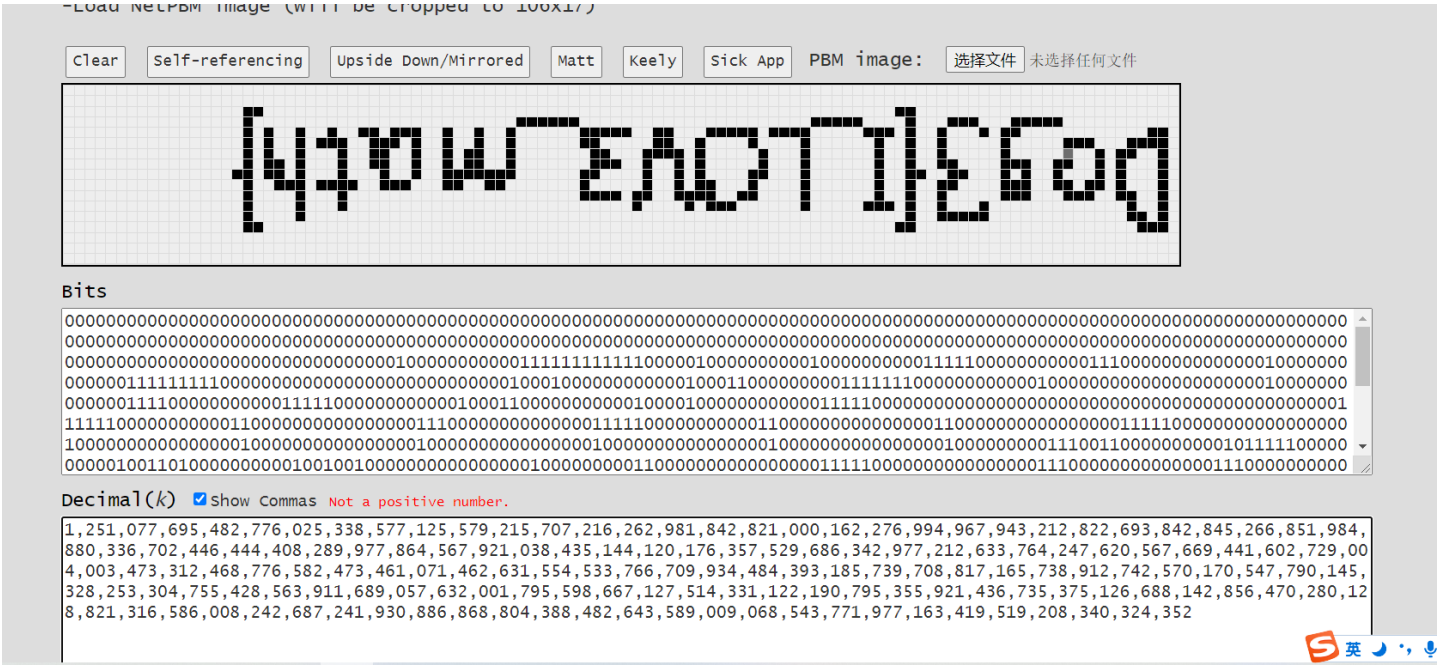
然后用QQ OCR一下

```
125107769548277602533857712557921570721626298184282100016227699496794321282269384284526685198488033670244644440828997786456792103843514412017635752968634297721263376424762056766944160272900400347331246877658247346107146263155453376670993448439318573970881716573891274257017054779014532825330475542856391168905763200179559866712751433112190795355921436735375126688142856470280128821316586008242687241930886868804388482643589009068543771977163419519208340324352
```

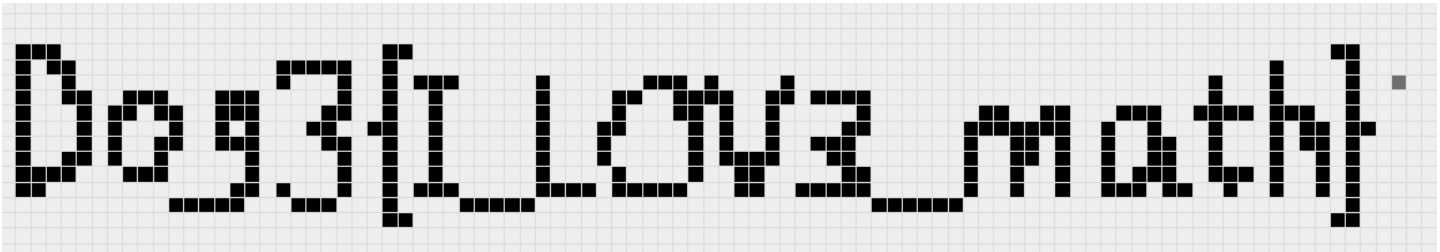
结合题目给的甚至能画出自己

找到了塔珀自指公式，然后github发现有解码的网站

http://keelyhill.github.io/tuppers-formula/



反过来看即可



```
D0g3{I_LOV3_math}
```

(img-r7kZPszo-1638081708605)]

反过来看即可

[外链图片转存中…(img-5botdHyY-1638081708608)]

```
D0g3{I_LOV3_math}
```