




2021安洵杯Misc writeup

原创

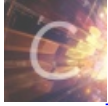
是Mumuzi  于 2021-11-28 14:42:34 发布  740  收藏 1

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

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/121591366

版权



[ctf](#) 专栏收录该内容

75 篇文章 28 订阅

订阅专栏

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



音乐私藏馆

发消息

这世界没有真正的感同身受(闲聊群: 9656684...

+ 关注 409.2万

弹幕列表

收起

时间	弹幕内容	发送时间
00:53	yellow	11-25 12:38
00:56	666	11-25 12:38
02:31	这一秒我眼眶真的湿润了	11-25 17:19
03:24	姆姆我想你了	11-25 17:32
02:18	卧槽卧槽	11-25 20:52
00:25	ohhhhhhhhhhhhhhhhhhhhh...	11-25 22:19
00:47	李耀华我爱你!	11-25 23:44
01:02	我爱死	11-26 00:56
00:25	D0g3{welcome_to_axbgogo...	11-26 11:31
05:18	想你	11-26 16:52
00:53	摇滚不止, 生命不息	11-26 18:07
02:17	上岸	11-26 20:58
02:24	相信自己	11-26 20:58
02:42	郑钧流星是翻唱yellow, 调...	11-26 22:14
00:57	李乐鸡戒了吧	11-26 22:15
02:21	这里的电吉他加上这个场景...	11-26 22:15
01:35	考研上岸	11-26 23:10

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)
```

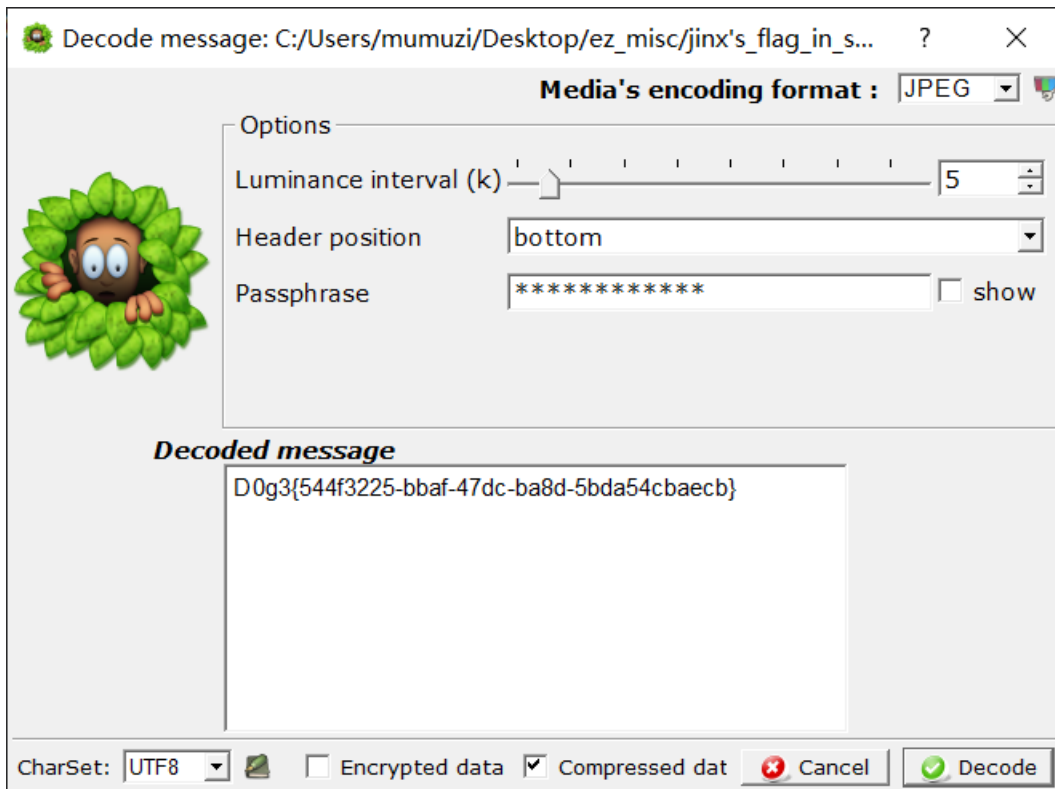
密码为AGdJfpqebmXpptloa

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

Scottie...



解码

MRPVI4TZL5K GK4TSGRZGSYJBPU=====

Output

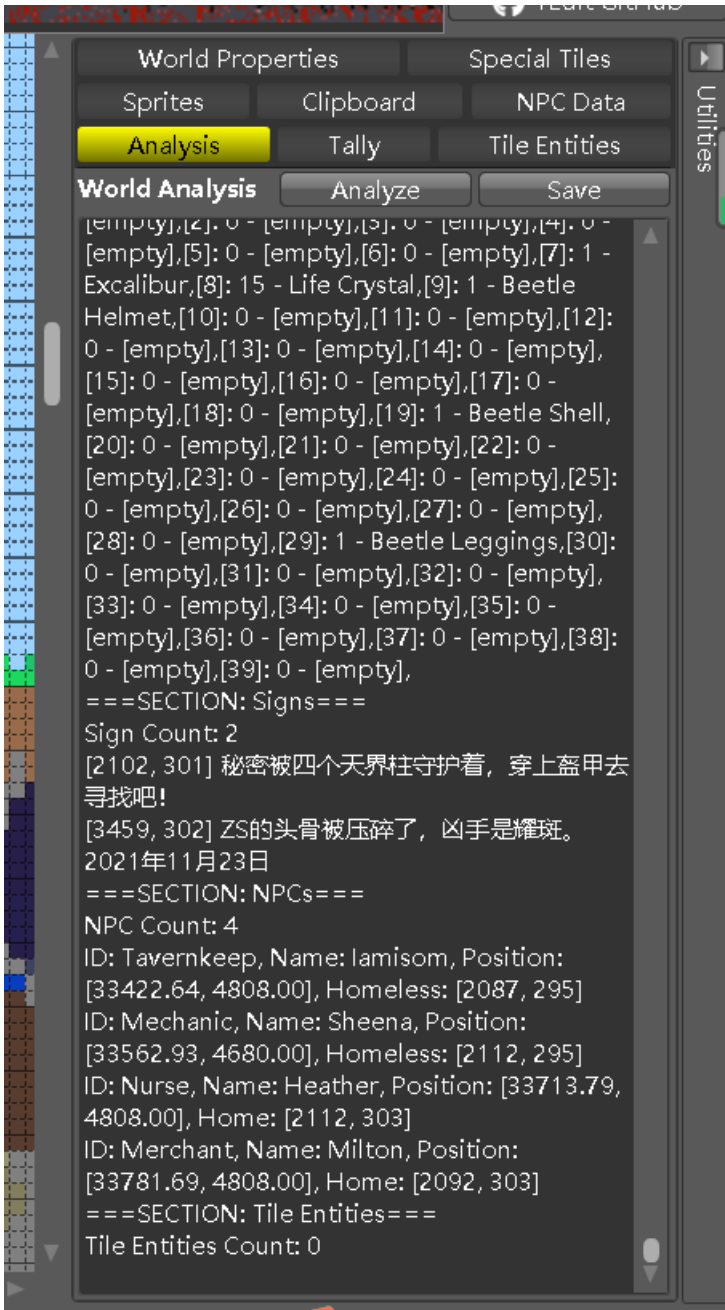
```
d_Try_Terr4ria!}
```

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74YF6QL0

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

```

10 [1213, 509] - Contents: [0]: 1 - ArcaneCloud in a Bottle,[1]: 1 - Suspicious Looking Eye,[2]: 5 - Gold Bar,[3]: 48 - Throwing Knife,[4]: 2 - Water Walking Potion,[5]: 2 - Teleportati
11 [1550, 693] - Contents: [0]: 1 - Boomstick,[1]: 1 - Suspicious Looking Eye,[2]: 1 - Dynamite,[3]: 41 - Throwing Knife,[4]: 2 - Archery Potion,[5]: 1 - Invisibility Potion,[6]: 1 - Go
12 [1668, 246] [8:16] - Contents: [0]: 1 - 'J' Statue,[1]: 1 - 'U' Statue,[2]: 1 - 'W' Statue,[3]: 1 - 'W' Statue,[4]: 1 - '4' Statue,[5]: 1 - '2' Statue,[6]: 1 - 'I' Statue,[7]: 1 - 'D'
13 [839, 288] [1:8] - Contents: [0]: 1 - 'I' Statue,[1]: 1 - 'Q' Statue,[2]: 1 - 'Y' Statue,[3]: 1 - 'G' Statue,[4]: 1 - 'O' Statue,[5]: 1 - 'M' Statue,[6]: 1 - '3' Statue,[7]: 1 - '3' Sta
14 [2582, 303] [16:23] - Contents: [0]: 1 - 'K' Statue,[1]: 1 - 'I' Statue,[2]: 1 - '2' Statue,[3]: 1 - 'G' Statue,[4]: 1 - 'M' Statue,[5]: 1 - '5' Statue,[6]: 1 - 'C' Statue,[7]: 0 - [er
15 [3408, 302] 原文已经被我拿走了-机械师sheena - Contents: [0]: 0 - [empty],[1]: 0 - [empty],[2]: 0 - [empty],[3]: 0 - [empty],[4]: 0 - [empty],[5]: 0 - [empty],[6]: 0 - [empty],[7]: 0 - [er
16 [2102, 293] - Contents: [0]: 0 - [empty],[1]: 0 - [empty],[2]: 0 - [empty],[3]: 0 - [empty],[4]: 0 - [empty],[5]: 0 - [empty],[6]: 0 - [empty],[7]: 1 - Excalibur,[8]: 15 - Life Cryst
17 ===SECTION: Signs===
18 Sign Count: 2
19 [2102, 301] 秘密被四个天界柱守护着, 穿上盔甲去寻找吧!
20 [3459, 302] ZS的头骨被压碎了, 凶手是耀斑。
21 2021年11月23日
22 ===SECTION: NPCs===

```

按顺序撸下来,得到

YQIGOM33JUW4ZLDKI2GM5C7I4YF6QL0

Output

Ä.g3{M1necR4ft_G0_A`

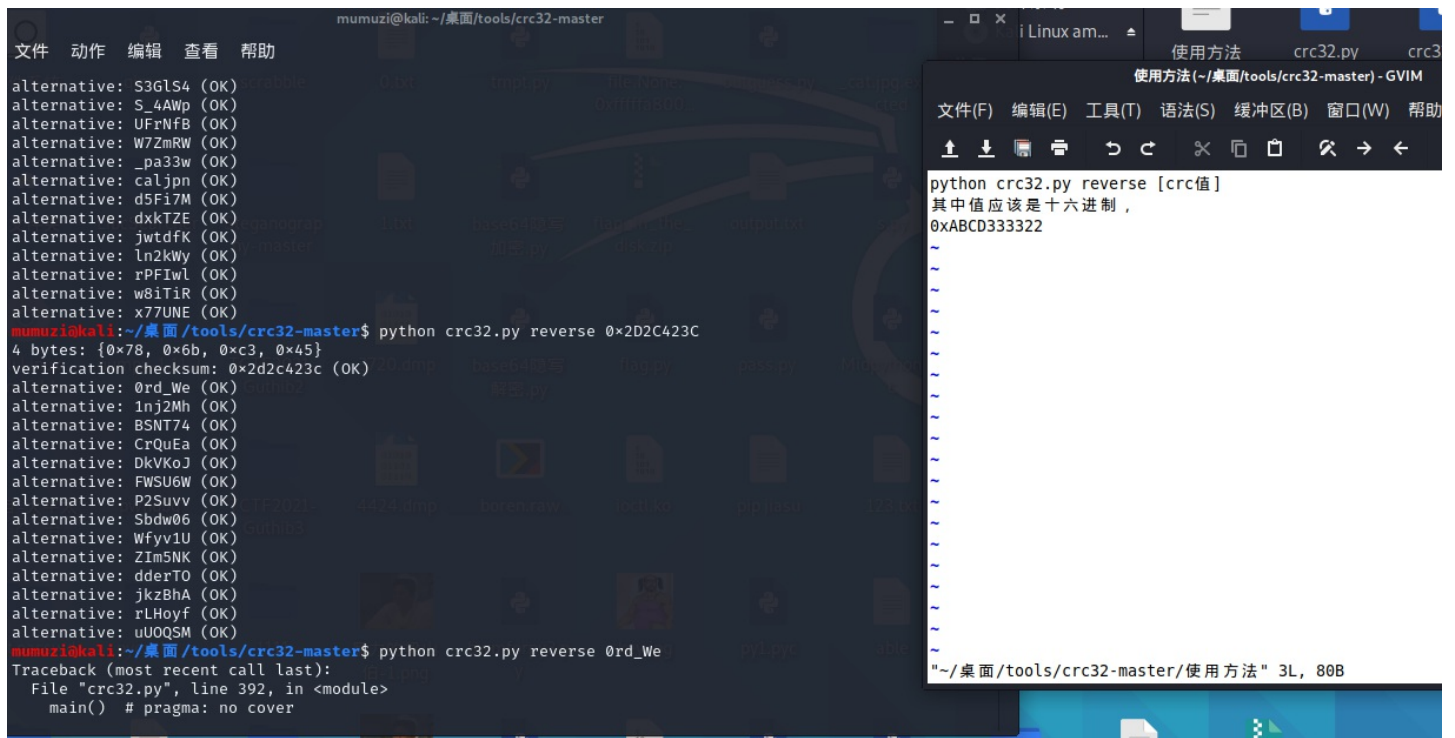
emm能看出来前面和后面都有错误，但是前面能知道是D0g3{M1necR4ft_G0_A 后面是d_Try_Terr4ria!}

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



```
mumuzi@kali: ~/桌面/tools/crc32-master
文件 动作 编辑 查看 帮助
alternative: S3GLS4 (OK)
alternative: S_4AWp (OK)
alternative: UFRnFB (OK)
alternative: W7ZmRW (OK)
alternative: _pa33w (OK)
alternative: caljpn (OK)
alternative: d5F17M (OK)
alternative: dxkTZE (OK)
alternative: jwtdfk (OK)
alternative: ln2KWy (OK)
alternative: rPFIwl (OK)
alternative: w8iTIR (OK)
alternative: x77UNE (OK)
mumuzi@kali:~/桌面/tools/crc32-master$ python crc32.py reverse 0x2D2C423C
4 bytes: {0x78, 0x6b, 0xc3, 0x45}
verification checksum: 0x2d2c423c (OK)
alternative: 0rd_We (OK)
alternative: 1nj2Mh (OK)
alternative: BSNT74 (OK)
alternative: CrQuEa (OK)
alternative: DkVKoJ (OK)
alternative: FWSU6W (OK)
alternative: P2Suvv (OK)
alternative: Sbdw06 (OK)
alternative: Wfyv1U (OK)
alternative: ZIm5NK (OK)
alternative: dderTO (OK)
alternative: jkzBhA (OK)
alternative: rLHoyf (OK)
alternative: uUOQSM (OK)
mumuzi@kali:~/桌面/tools/crc32-master$ python crc32.py reverse 0rd_We
Traceback (most recent call last):
  File "crc32.py", line 392, in <module>
    main() # pragma: no cover

Linux am...
使用方法  crc32.py  crc3
使用方法(~/桌面/tools/crc32-master) - GVIM
文件(F) 编辑(E) 工具(T) 语法(S) 缓冲区(B) 窗口(W) 帮助
python crc32.py reverse [crc值]
其中值应该是十六进制，
0xABCD333322
~/桌面/tools/crc32-master/使用方法" 3L, 80B
```

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

```

1251077695482776025338577125579215707216262981842821000162276994967943212822693842845266851984880336702446444408
2899778645679210384351441201763575296863429772126337642476205676694416027290040034733124687765824734610714626315
5453376670993448439318573970881716573891274257017054779014532825330475542856391168905763200179559866712751433112
2190795355921436735375126688142856470280128821316586008242687241930886868804388482643589009068543771977163419519
208340324352

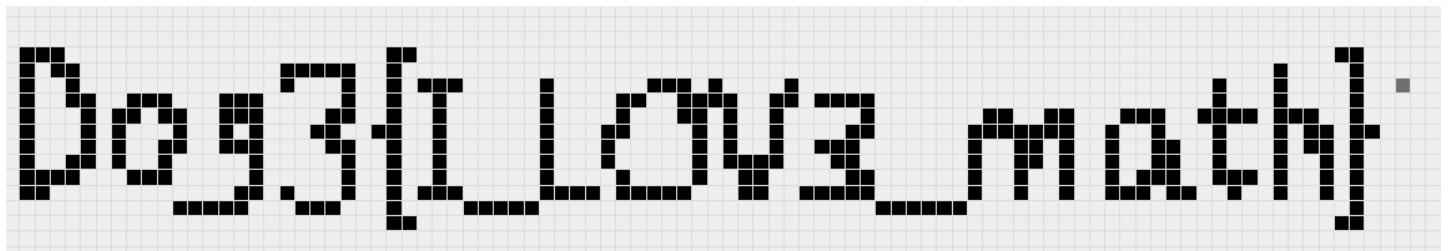
```

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-r7kZPso-1638081708605)]

反过来看即可

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

D0g3{I_LOV3_math}