

SUSCTF2022 misc wp

原创

vlan103 已于 2022-03-01 07:30:54 修改 2409 收藏 1

文章标签: [wp](#)

于 2022-02-28 23:43:16 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_51652400/article/details/123185105

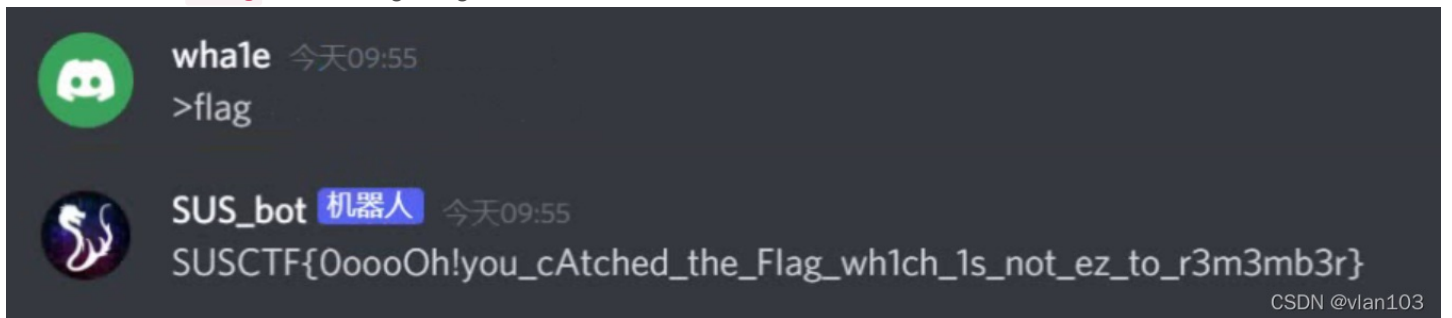
版权

文章目录

- [checkin](#)
- [AUDIO](#)
- [misound](#)
- [ra2](#)
- [Tanner](#)

checkin

私信机器人发送 `>flag` 即可获得flag, flag会瞬间换成其他消息, 截屏来不及就直接录频然后放0.1倍数看就行了。

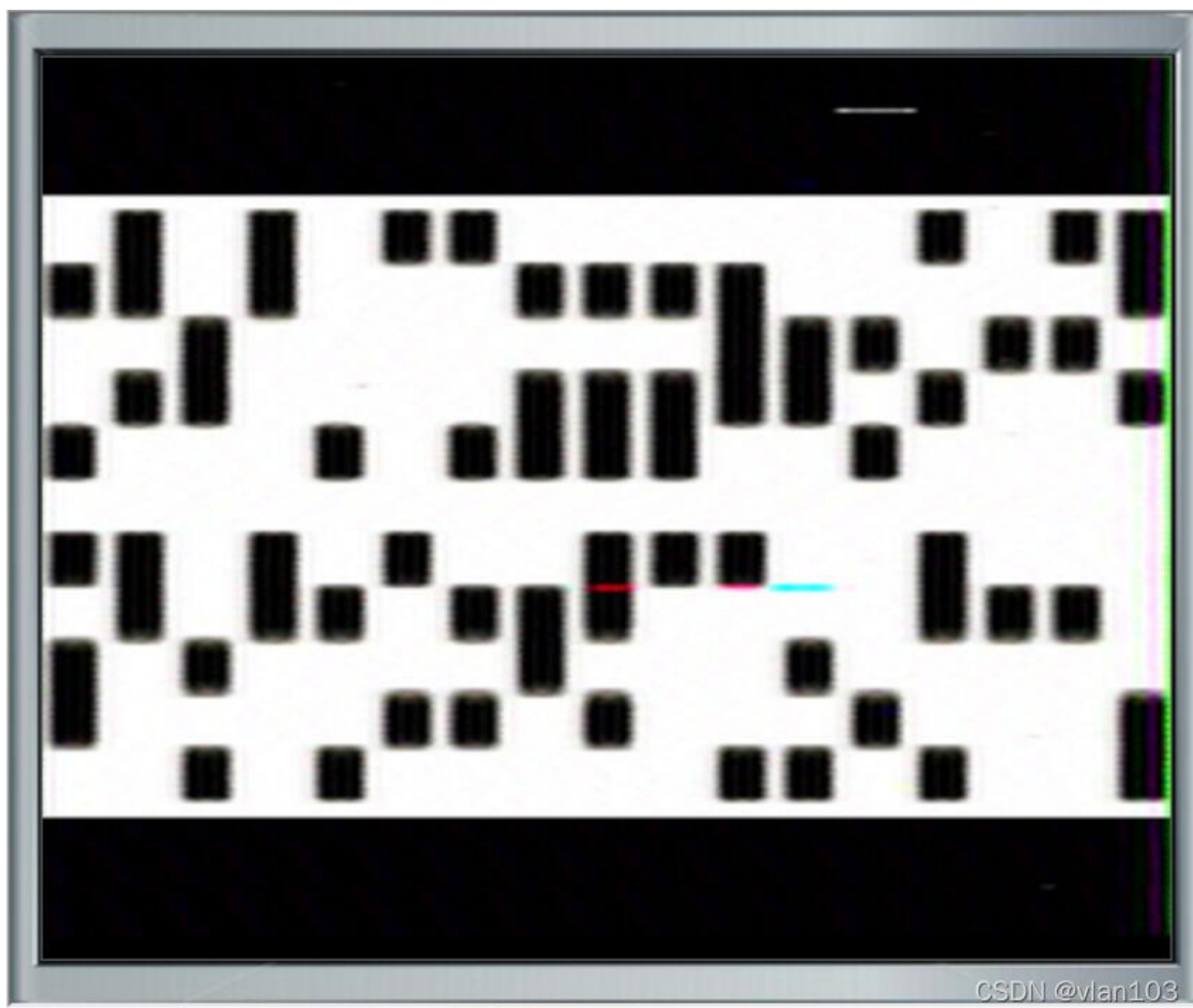


AUDIO

题目给了两段音频, 音乐与时长相同, 但 `fromfriends.wav` 在副歌部分比 `origin.mp3` 多了一段摩斯码, 然后通过像大佬学习可知如何操作

- au或者studio one之类的
- 音频处理软件
- 伴奏全选反相
- 然后调整音量大小
- 到互相抵消

接下来就是展示刀工的时候，把字符串区域切除，还原SSTV图片，这里我切的比较歪所以直接用C0oola的（刀法一流）



起初以为是转换成01之类的，但是没想到这是符号密码

<https://www.dcode.fr/dotsies-writing>

因为不知道顺序，所以横竖版本如下：

横：NQHFEOUUUShLMCJQRFLFNMGQAOLDWBBI

竖向：NRQFHLFFENAMOKUGUQUASOHLDDMWCBJBQI

结果非预期直接跳过该key解出

```
num1 = [207, 359, 220, 224, 352, 315, 359, 374, 290, 310, 277, 507, 391, 513, 423, 392, 508, 383, 440, 322, 420,
427, 503, 460, 295, 318, 245, 302, 407, 414, 410, 130, 369, 317]
num2 = "AnEWmULTiPLyis_etimes_wiLLbEcomE_B"
for i in range(34):
    flag = (num1[i]*26 + 1) / ord(num2[i])
    print(chr(round(flag)), end="")
```

这里又问了一遍出题人，出题人表示SSTV转出来的key是有用的。

留一个坑回头补上

ra2

正常来讲应该是可以修改游戏代码的，文件路径 `Romanovs-Vengeance\mods\rv\maps\ctf-01`，但是尝试多次修改都没成功，于是就硬玩了。

游戏手残党表示看不懂英文并且不理解游戏导致花了很多时间，枯先造围墙把家围起来，然后就可以满世界浪了

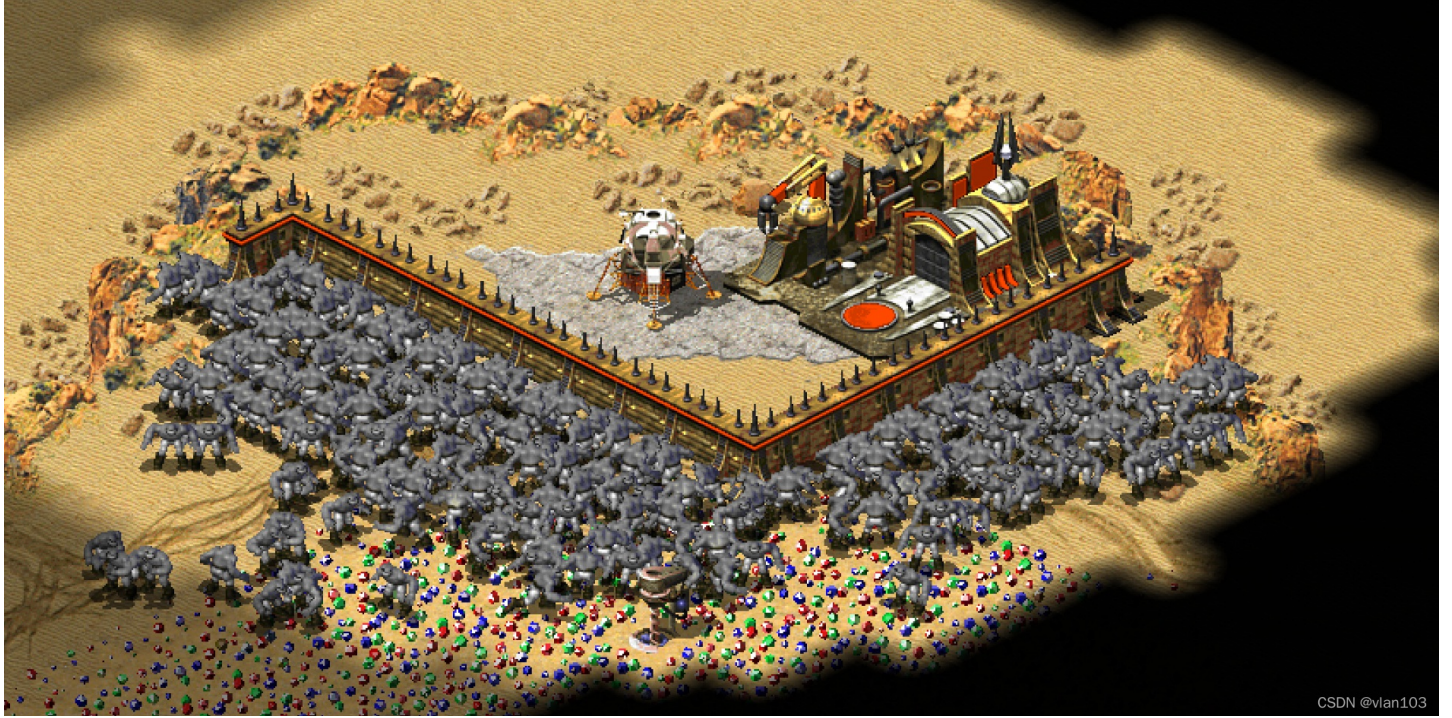


找了大半个世界最后发现就在家下面（该图是）



回到家正下方就发现了这个会动的牌子，上面就是flag，截屏太麻烦就老办法录个频暂停看，结束。





Tanner

不会写，留一个坑。