【T-Star赛事笔记】腾讯安全应急响应中心（TSRC）+WriteUp赛题四+比赛评价+小彩蛋--by wjl110

原创

爬虫数据分析师 已于 2022-04-26 21:10:51 修改 158 收藏

分类专栏： ctf 学习笔记 渗透笔记 文章标签： web安全 网络 安全

于 2022-04-26 21:00:46 首次发布

前言：

(,･∀･)ﾉ゛hello，不出意外,各位小伙伴已经完成了这次的T-Star赛事,不知道各位心情如何(我反正觉得比赛很nice),体验不错,就像是周末跟小伙伴去玩儿密室逃脱一样,惊险刺激哈哈哈哈哈,下面□是我在解第四题的思路和方法,提供给各位小伙伴参考,最近在练听力,所以摩斯密码纯考听滴~哈哈哈哈,听说还有别的小伙伴用在线音频文件解密的方式也是可以滴，方便快捷–，let's go~~~

0x01赛题描述

跳转下载zip

```
http://175.178.148.197/b378603d0266d73e743c8d05f5bc3ebe.zip
```

提示

> 需要修复二维码与压缩包，分析出压缩包密码，答案为解压后的TXT内容

0x02解压缩zip包

解压缩zip包后，得到两个文件，第一个是二维码，第二个是压缩包zip

修复第一个二维码文件

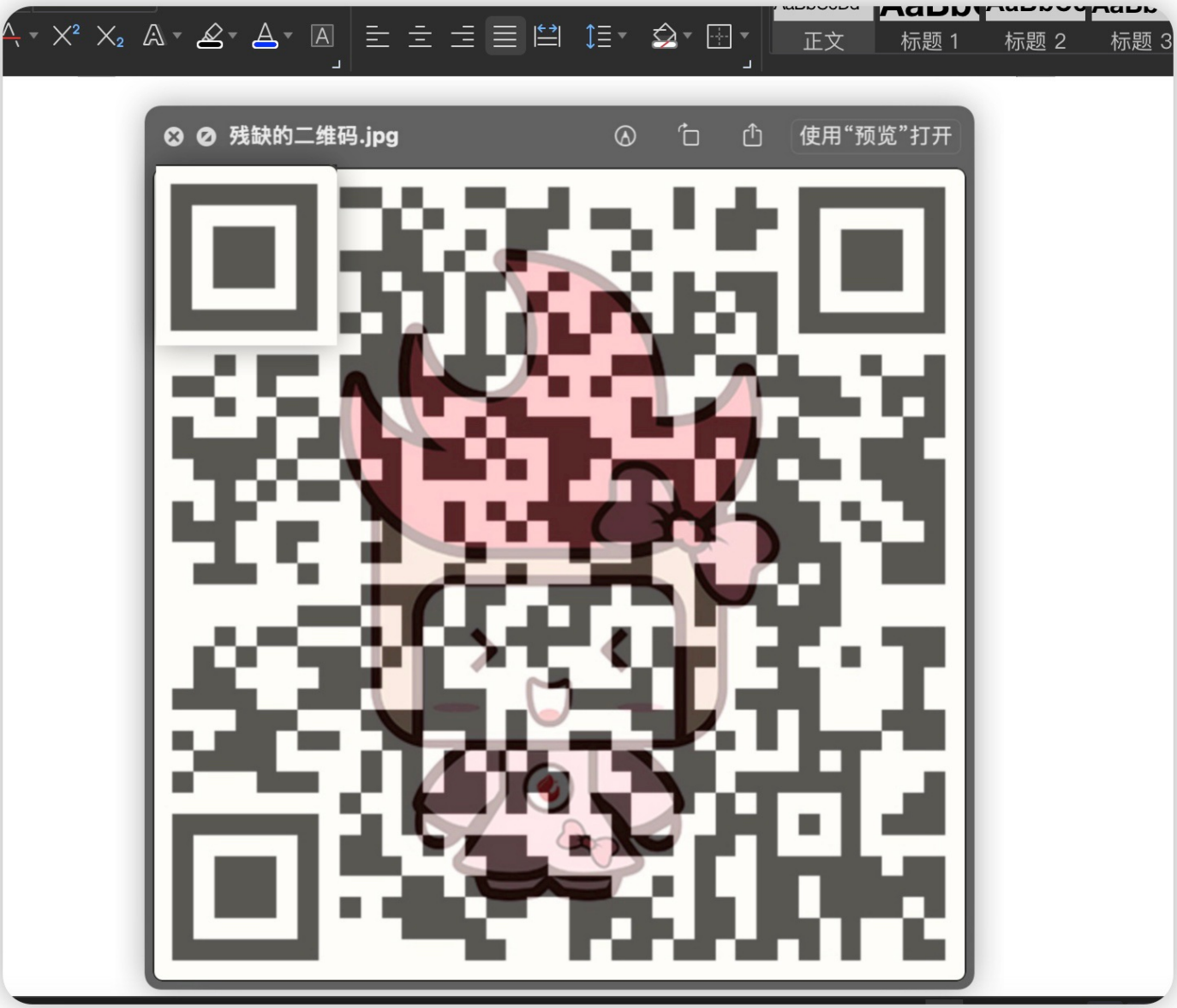
> 我在此是将其截图放置于WPS的word文档内

分析可以知道二维码构造由三个（左上、左下、右上）相同部分组成，此图缺失左上角部分。

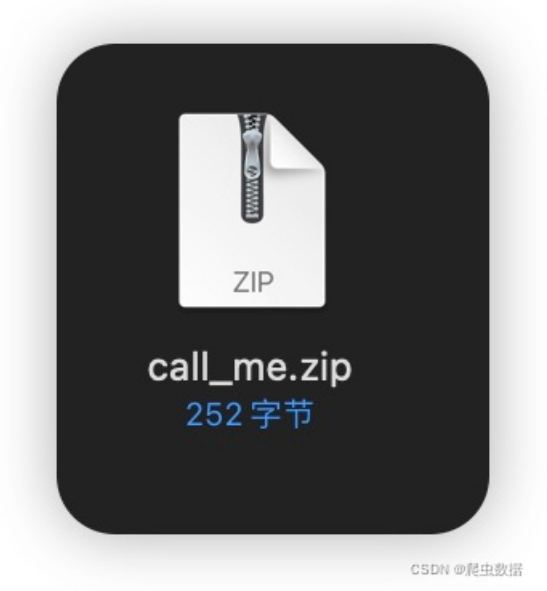
将右上角截取出来，拼凑到左上，如下图所示。

截取右上角

拼凑左上角



扫描二维码后得到一个zip文件



打开需要解压密码

此时将思路转到第二个“破镜重圆”压缩包

0x03解压缩zip包

解压报错，将其用VScode自带的hex editor编辑器打开zip文件查看hex编码并分析原因

Tips:

> 压缩文件头数据区hex
> 50 4B 03 04：这是头文件标记为zip文件
> 14 00：解压文件所需 pkware 版本
> 00 00：全局方式位标记（有无加密） 头文件标记后2bytes
> 08 00：压缩方式
> 5A 7E：最后修改文件时间
> F7 46：最后修改文件日期
> 16 B5 80 14：CRC-32校验（1480B516）
> 19 00 00 00：压缩后尺寸（25）
> 17 00 00 00：未压缩尺寸（23）
> 07 00：文件名长度
> 00 00：扩展记录长度

分析可知第二位错误，将其更改为4B，然后保存，解压缩zip包，得到一个.mp3文件

0x04对.mp3文件进行分析

播放后发现是一段**摩斯密码**

对比摩斯密码对照图表可以将其内容复现出来

1{-— — — —} 2{--— — —} 3{---— —} 4{----—} 5{----} 6{—----} 7{— —---} 8{— — —--} 9{— — — —-} 0{— — — — —}	A{-—}滴答　　B{—---}答滴滴滴 C{—-—-}答滴答滴　　D{—--}答滴滴 E{-}滴　　F{--—-}滴滴答滴 G{——-}答答滴　　H{----}滴滴滴滴 I{--}滴　　J{-———}滴答答答 K{—-—}答滴答　　L{-—--}滴答滴滴 M{——}答答　　N{—-}答滴 O{———}答答答　　P{-——-}滴答答滴 Q{——-—}答答滴答　　R{-—-}滴答滴 S{---}滴滴滴　　T{—}答 U{--—}滴滴答　　V{---—}滴滴滴答 W{-——}滴答答　　X{—--—}答滴滴答 Y{—-——}答滴答答　　Z{——--}答答滴滴

-==== 1

====- 9

====- 9

-==== 1

===== 0

---== 3

===--8

=----6

==---7

====- 9

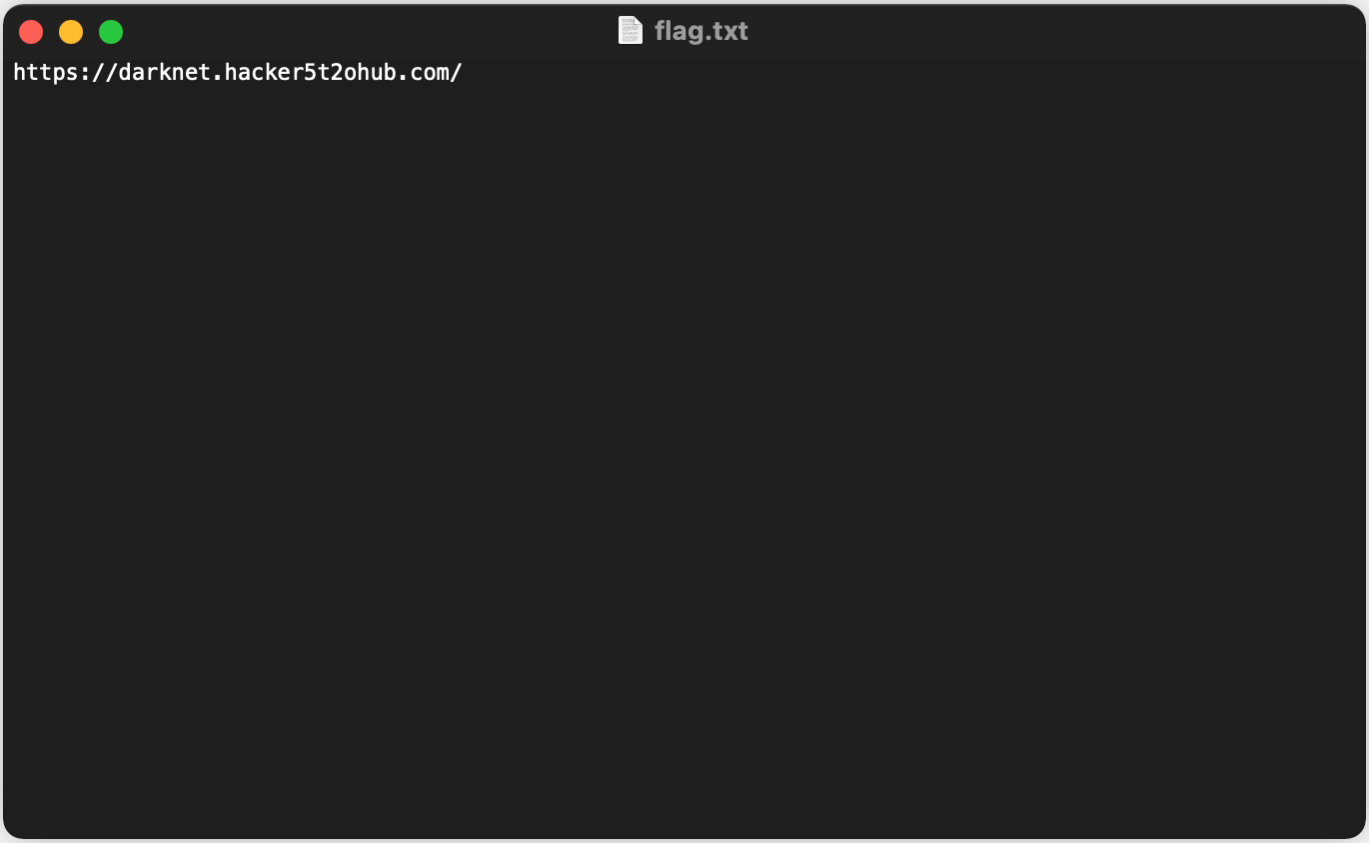
==---7

19910386797

得到密码**19910386797**

0x05解压后得到flag

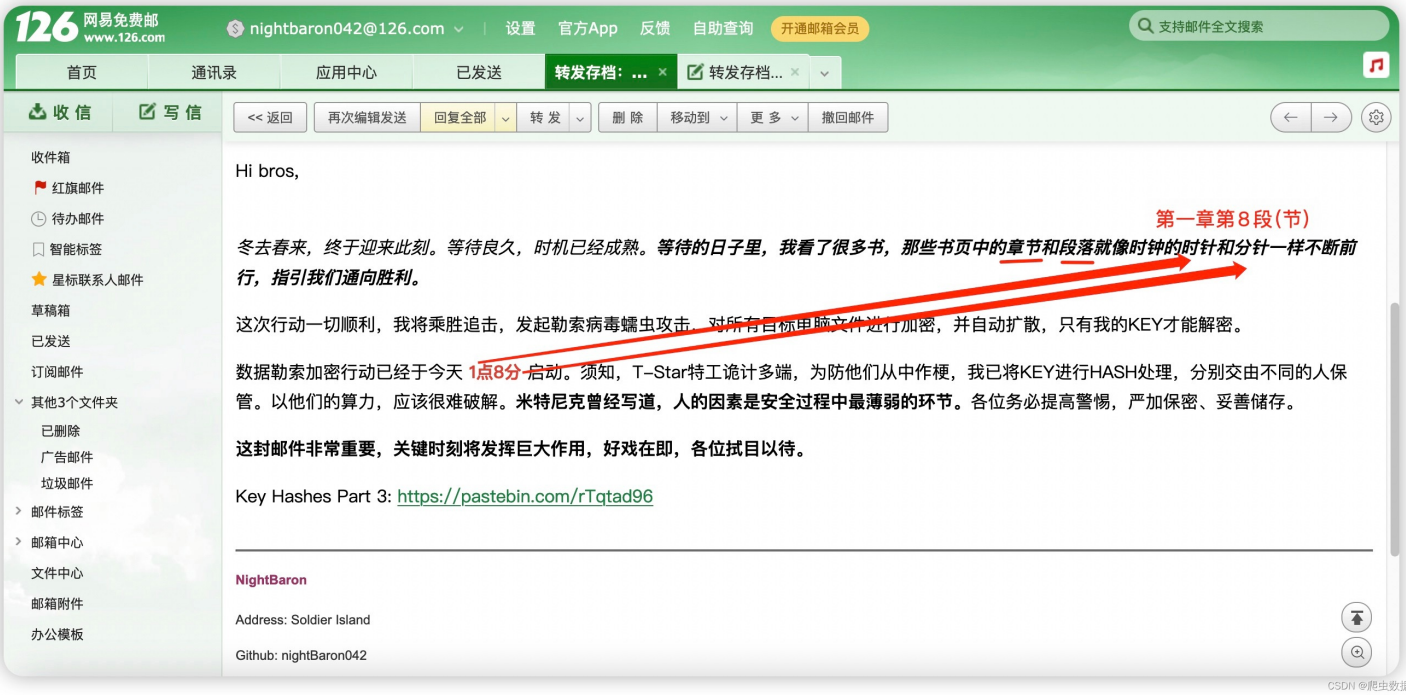
将得到的密码输入得到flag.txt文件



flag：

https://darknet.hacker5t2ohub.com/

比赛小彩蛋：



书名：《反欺骗的艺术：世界传奇黑客的经历分享》

夜男爵042

跟随

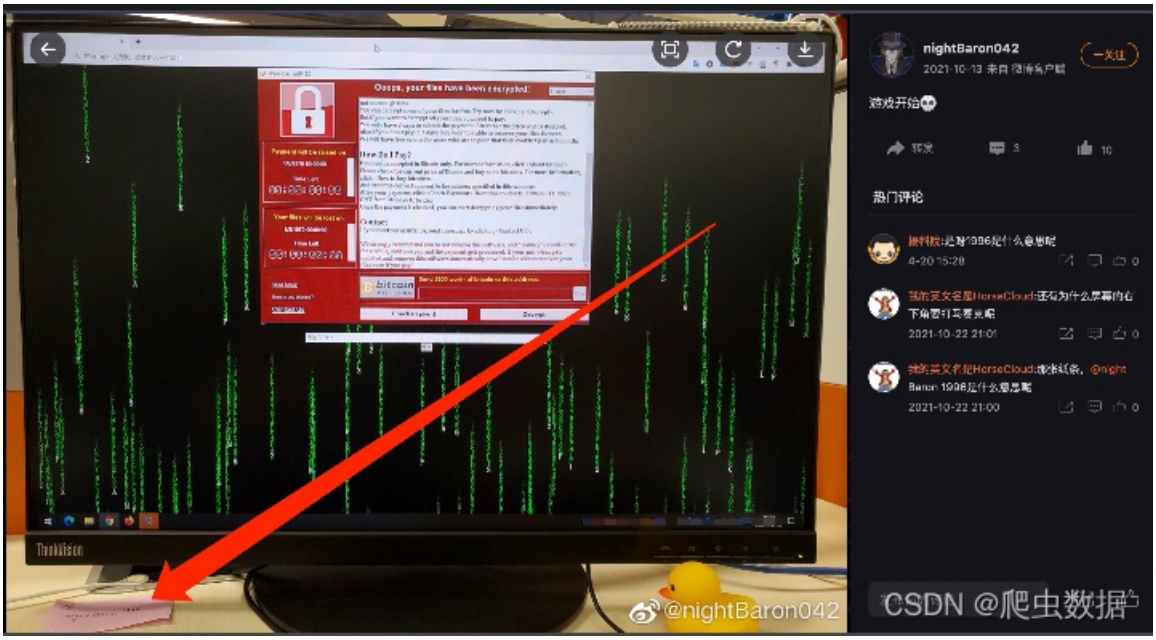
微博：nightBaron042

17 位关注者 · 0位 关注 者

nightbaron042@126.com

阻止或报告

匿名者的微博（邮箱密码）



匿名者的微博（邮箱密码）

比赛评价:

优点：

1、比赛有序进行，中途未出现服务器宕机等严重问题。（除了第一个题有许多小伙伴可能不知道做法，用扫描器导致服务器拥堵以外，剩下5道题的体验很好~）

2、开放实时排行榜的功能，能让小伙伴们实时了解自己的答题rank情况，清楚明了~

3、比赛时间合适，能给小伙伴足够的时间去解题，去学习，去探索

需改进地方和一些建议：

1、提供一个大数据可视化屏幕，将小伙伴解题first blood ，second blood等在可视屏上展出，将题目的解出人数进行统计~

2、比赛前提前开放服务器入口测试服务器压力和阈值（防cc攻击，ban ip 等），再根据预期人数进行调整和配置优化~

3、关于剧情内容上，建议可以丰富一下，多用解密和蛛丝马迹探寻的方法，例如我在nightbaron042的微博，github等地方找到的彩蛋等等~

此次比赛很给力，期待举办方下一次的举办（公众号里蹲tsrc，希望能多多举行类似比赛,主要是开心啦~）

——end