2022 SMUCTF 永远都对-rui WriteUp

原创

瑞瑞z 于 2022-04-20 17:01:57 发布 1006 收藏
分类专栏： CTF 文章标签： web安全

Misc

签到

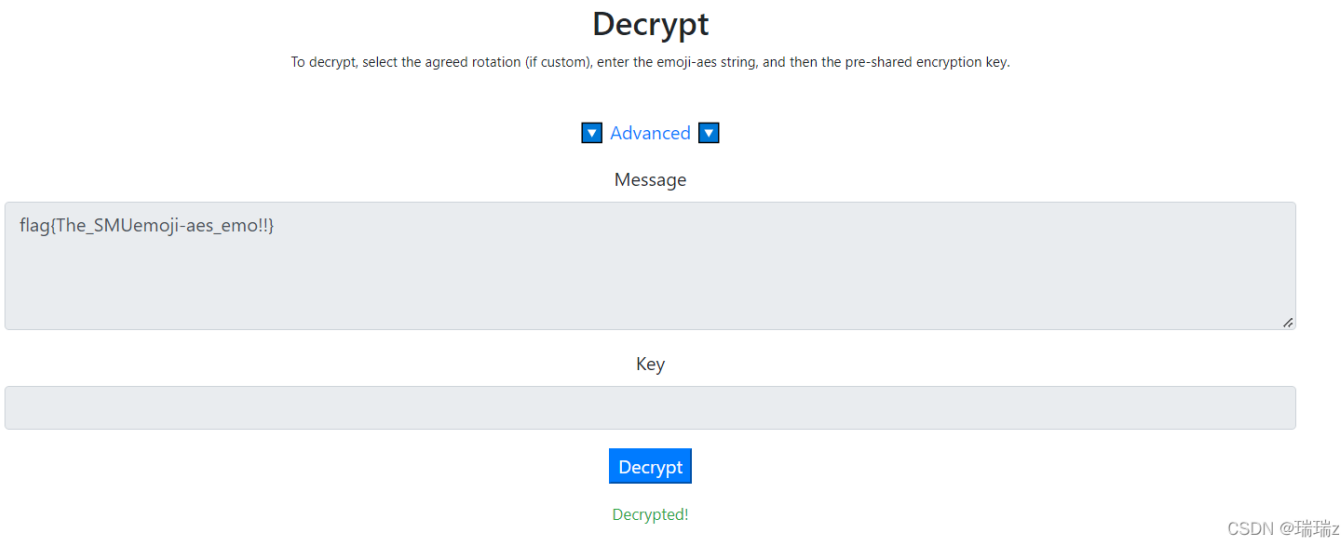
直接输入flag。

emoji

> □□□□□□□□□□□□□☃□☺□□□□□□□☀□□□□□□□□□□□☺□☺□□☃□□□□□□☀□☂□✖□□□□□✉□□□□□□□□
> 出题人给我发了这串表情，说了SMUCTF，这是什么意思？

把emoji和key复制到 emoji-aes 解密得到flag

（key 就是 SMUCTF）

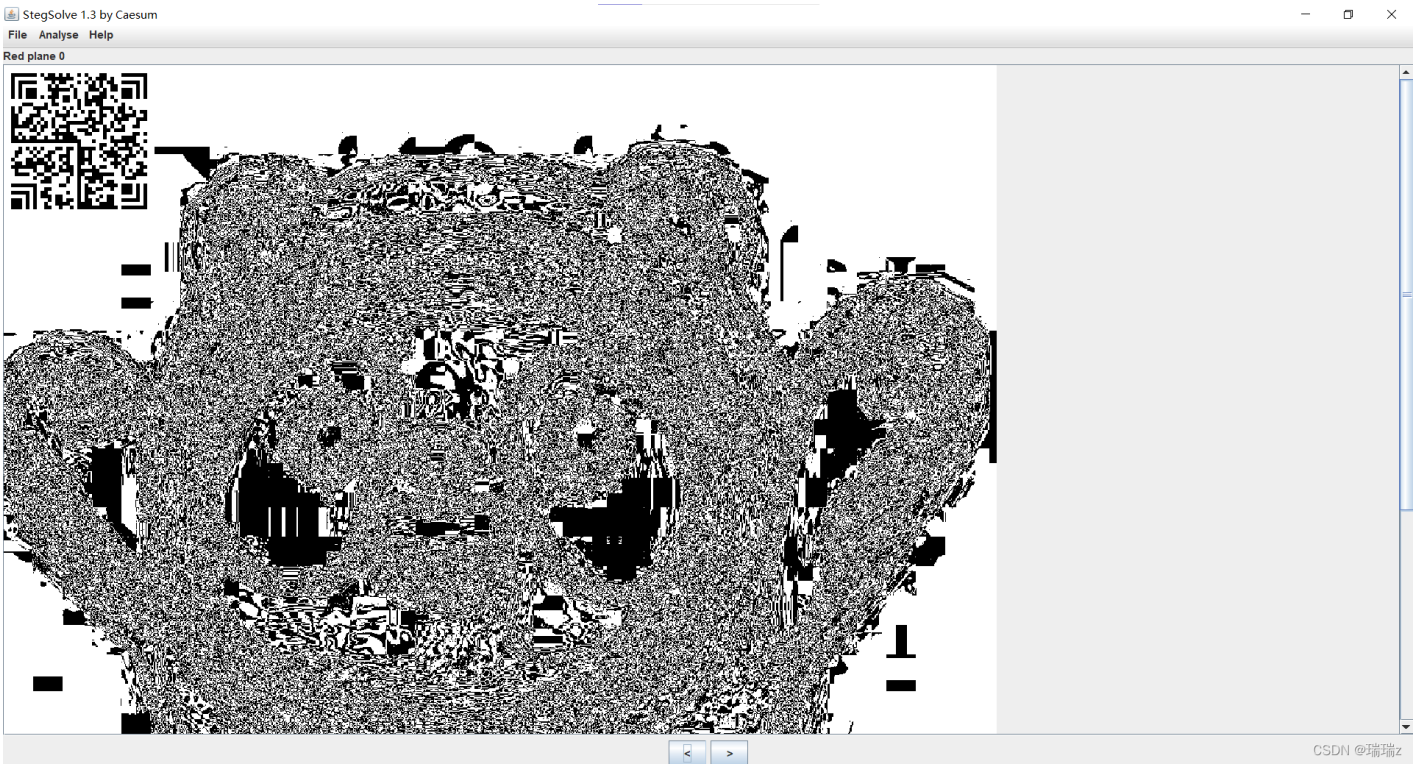


SMUGIFQR

> 题目附件给了一个gif的二维码，分别扫出每一个二维码组合即可得到flag。

冰墩墩的汉信码

把冰墩墩图片放到StegSolve里得到汉信码

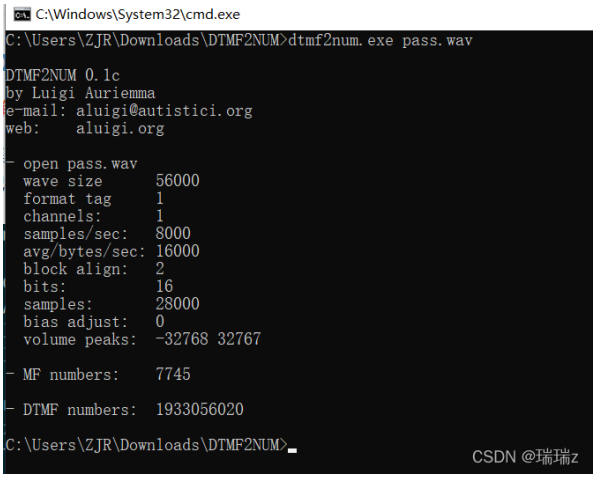


扫码即可得到flag

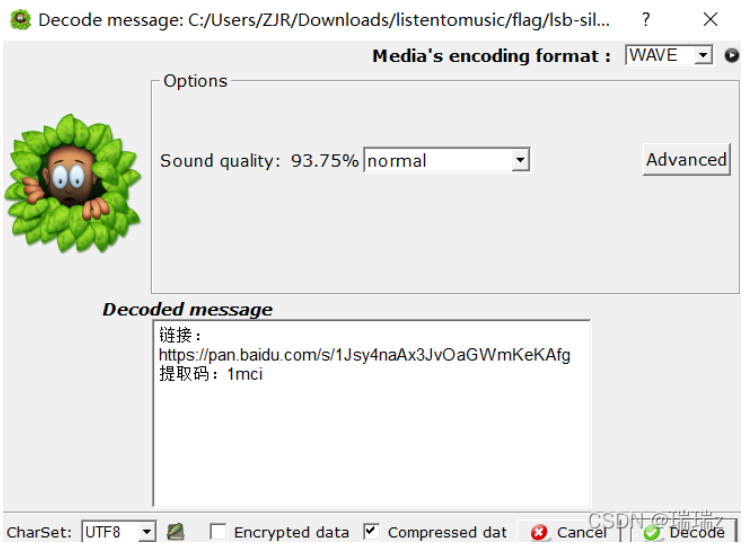
listentomusic

> 题目给了一段拨号音与一个加密的压缩包

拨号音用DTMF2NUM解出后得到压缩包密码



打开压缩包后发现里面还有一首歌，先用了Audacity查看频谱图没有得到线索，我又用了SilentEye打开，得到了一个百度网盘的链接

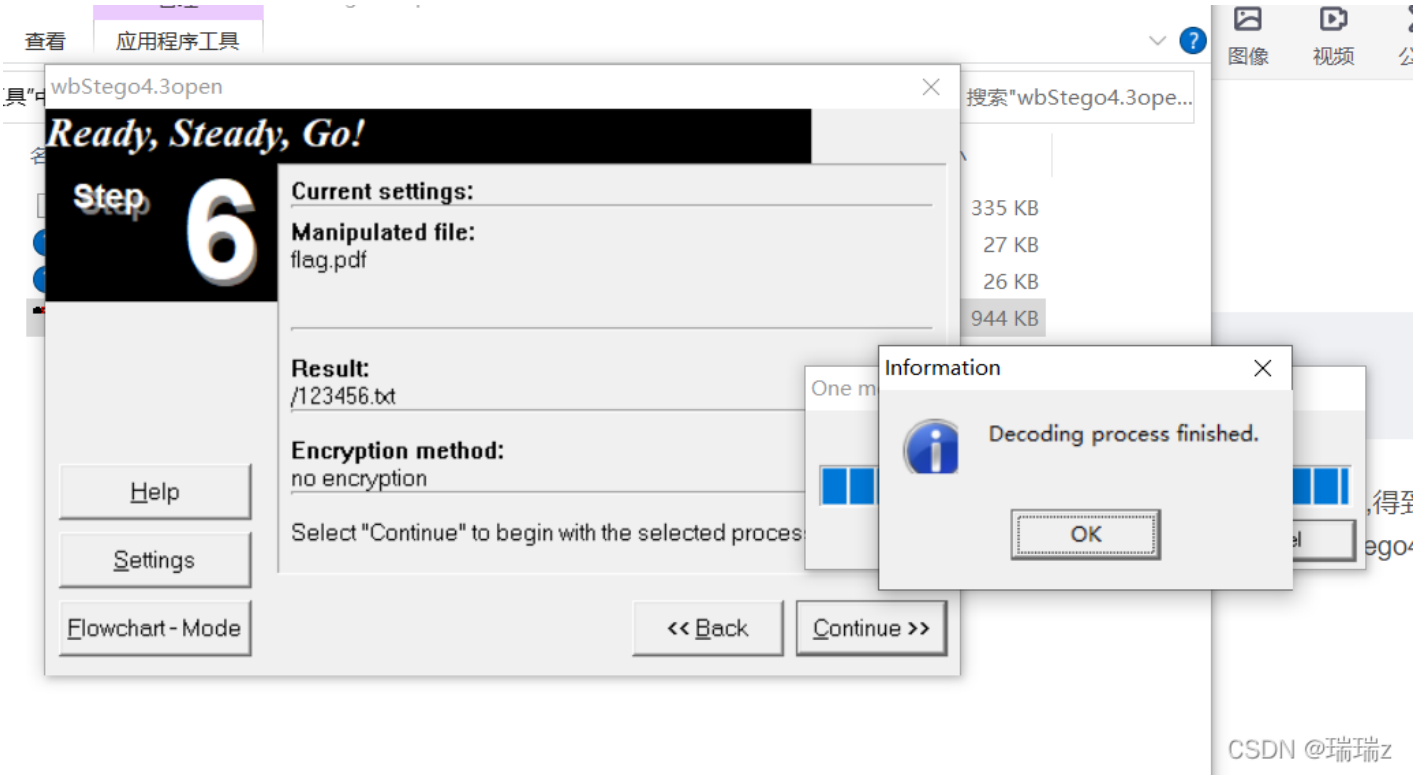


链接里又是一段音频，发现这是慢扫描SSTV，在kali中用QSSTV接收得到flag

High-level_SMUpdf

> 题目给了一个加密的压缩包，里面有两个pdf

首先尝试密码爆破，其中一个pdf成功破解，发现是一篇文档，将其转成excel,得到flag.pdf的密码。打开flag.pdf里面是一个ppt并没有flag。这里想到应该是pdf隐写，用wbStego4.3open解密一下，得到flag。

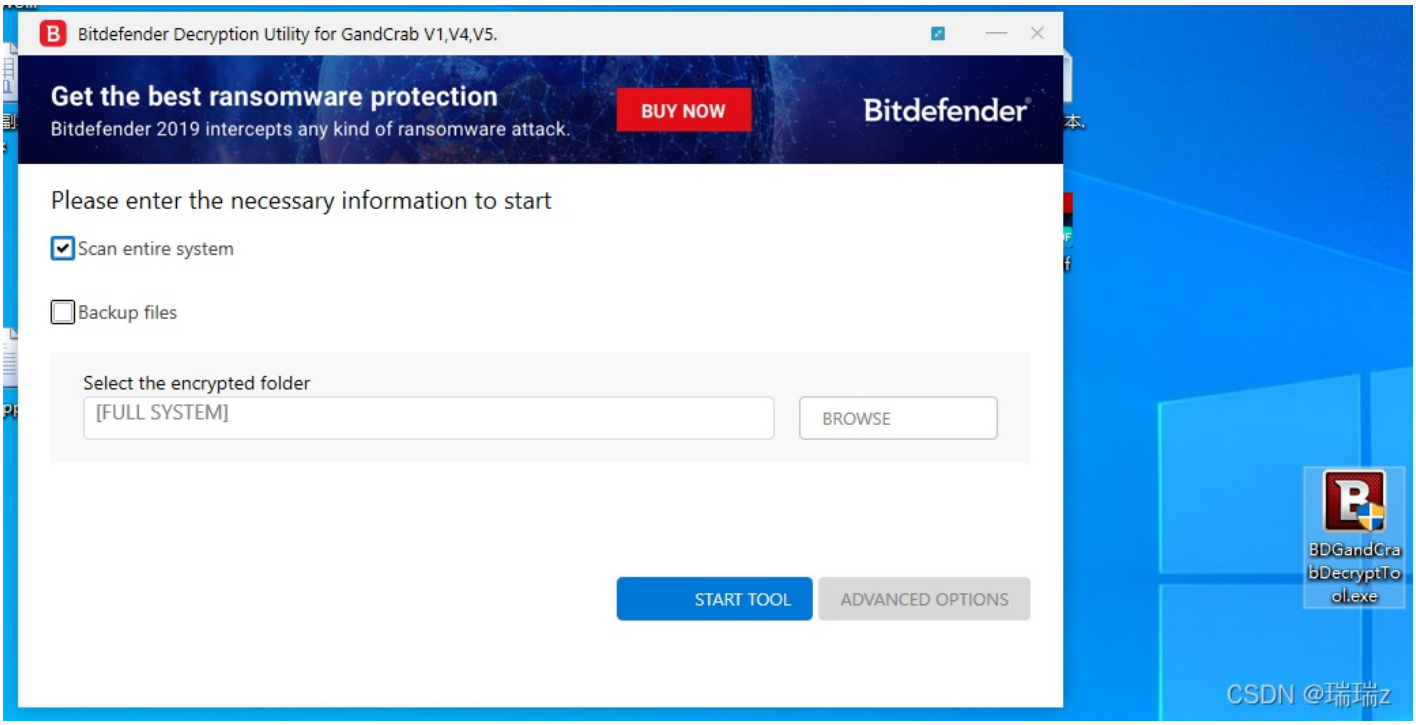


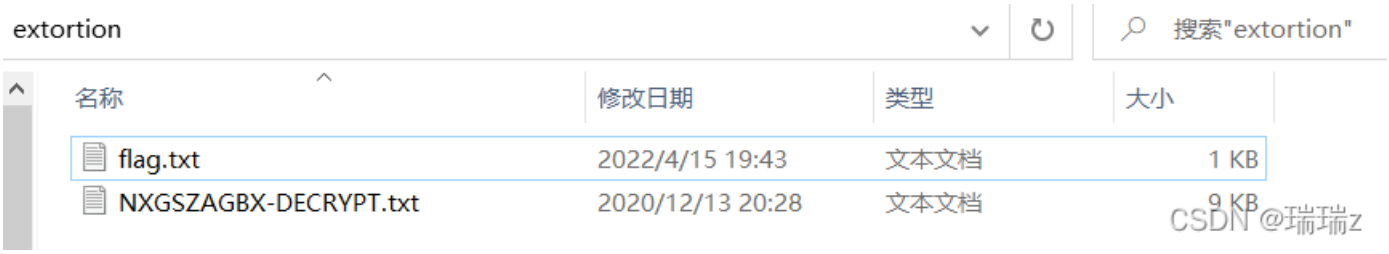
> flag{0urSMUPDF}

病毒文件恢复

> 题目描述：
>
> 三明学院网络安全协会内部出现了勒索病毒，并且各位的重要工程文件都被黑客锁住，请各位SMUCTFers解锁被勒索病毒锁住的文件。

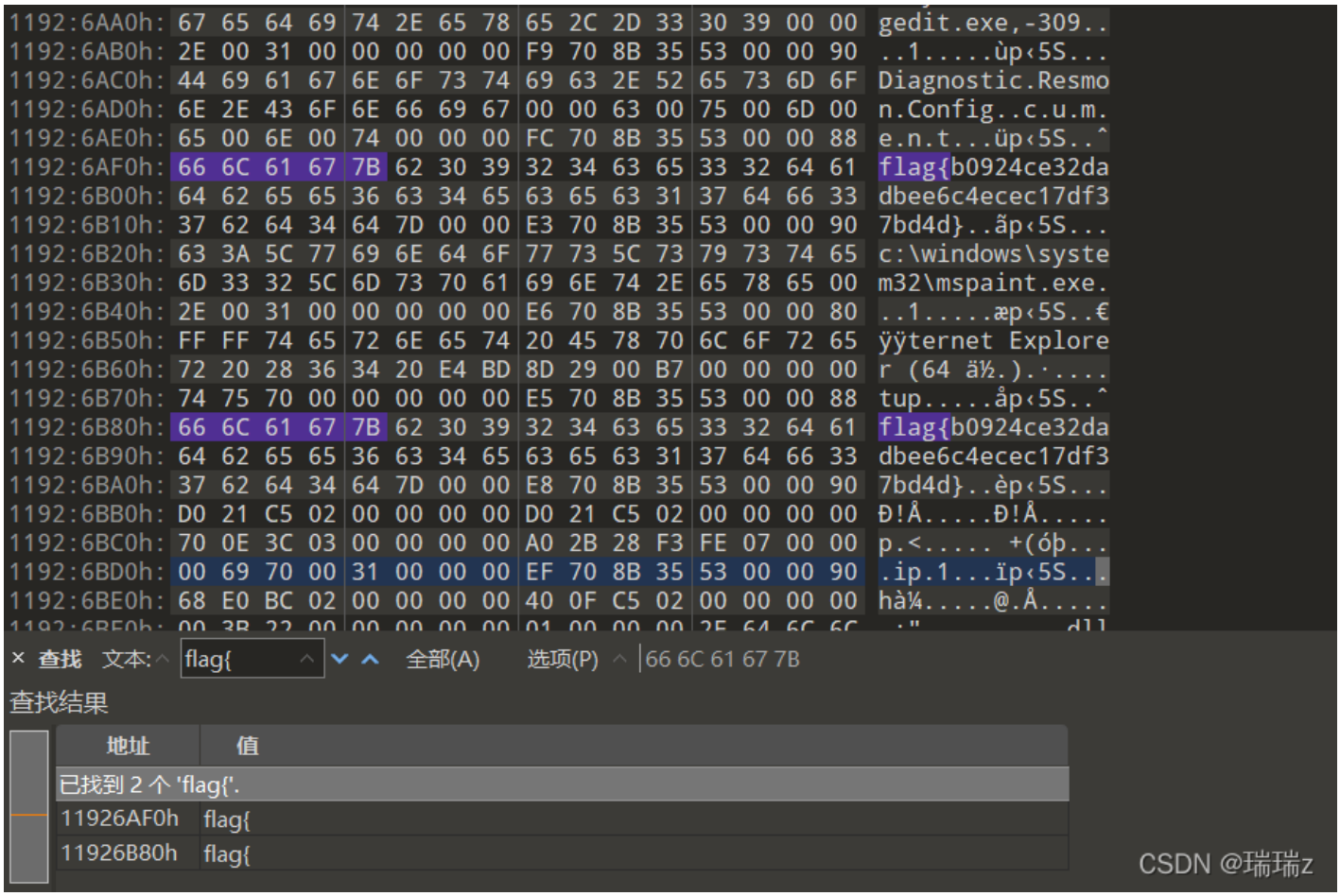
查看附件后发现该病毒为---=　GANDCRAB V5.1　=---，找到对应的解密工具BDGandCrabDecryptTool进行解密，即可得到flag





内存取证

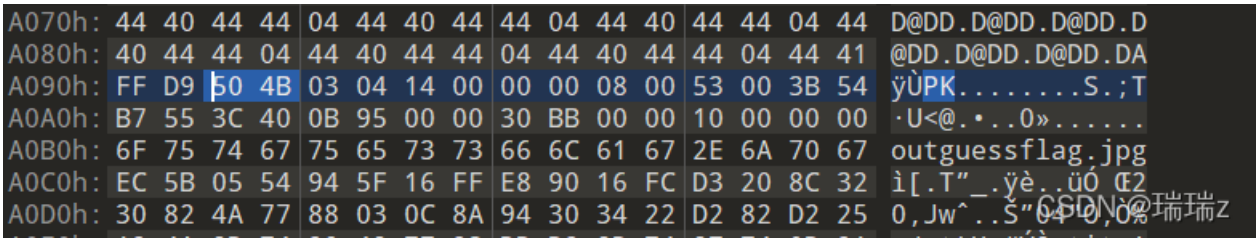
下载附件得到 WIN.raw文件，文件居然有512M。首先打开010Editor看一下，并没有发现文件头，直接在010里搜索文本“ flag{ ”，得到flag。



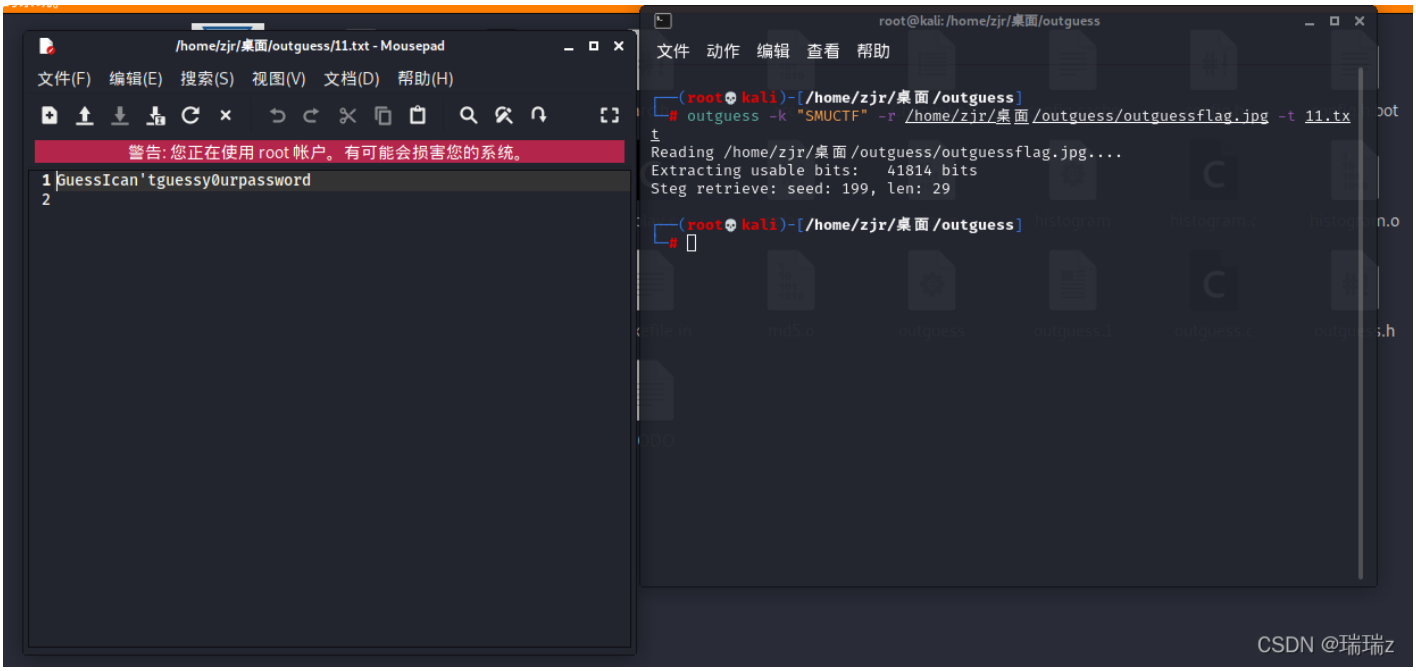
smuimg

这个题只给出了一张jpg的图片，看似没有任何线索，在010Editor中打开后发现别有洞天。

居然在文本栏中发现了PK，50 4B 03 04 这不是zip的文件头吗。原来这张图片背后隐藏了一个压缩包。

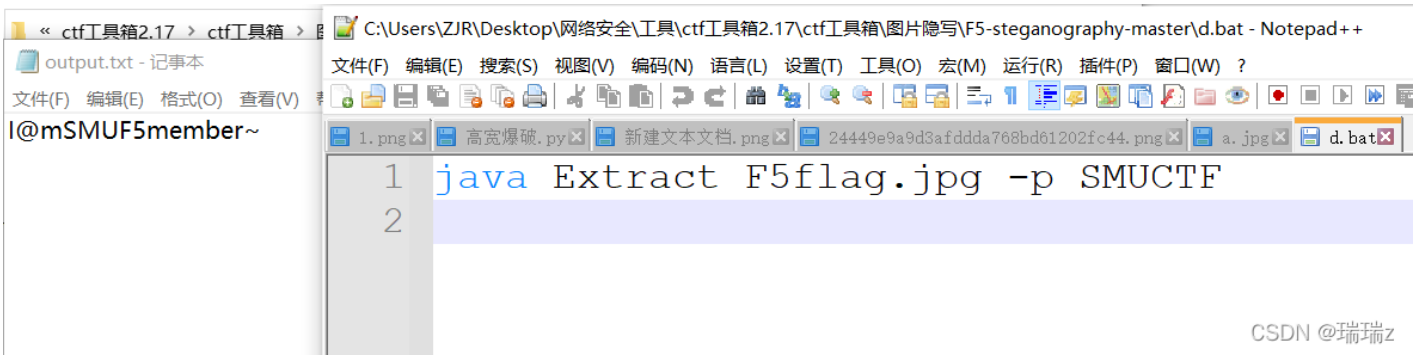


分离图片与压缩包后，将其解压缩，又得到了一张图片与一个加密的压缩包。显而易见这个压缩包的密码肯定在这张图片里。既然图片的名字叫outguessflag.jpg，那就试试outguess隐写吧。在kali里打开outguess，别忘了压缩包注释里还有一行SMUCTF，那这个应该就是key。



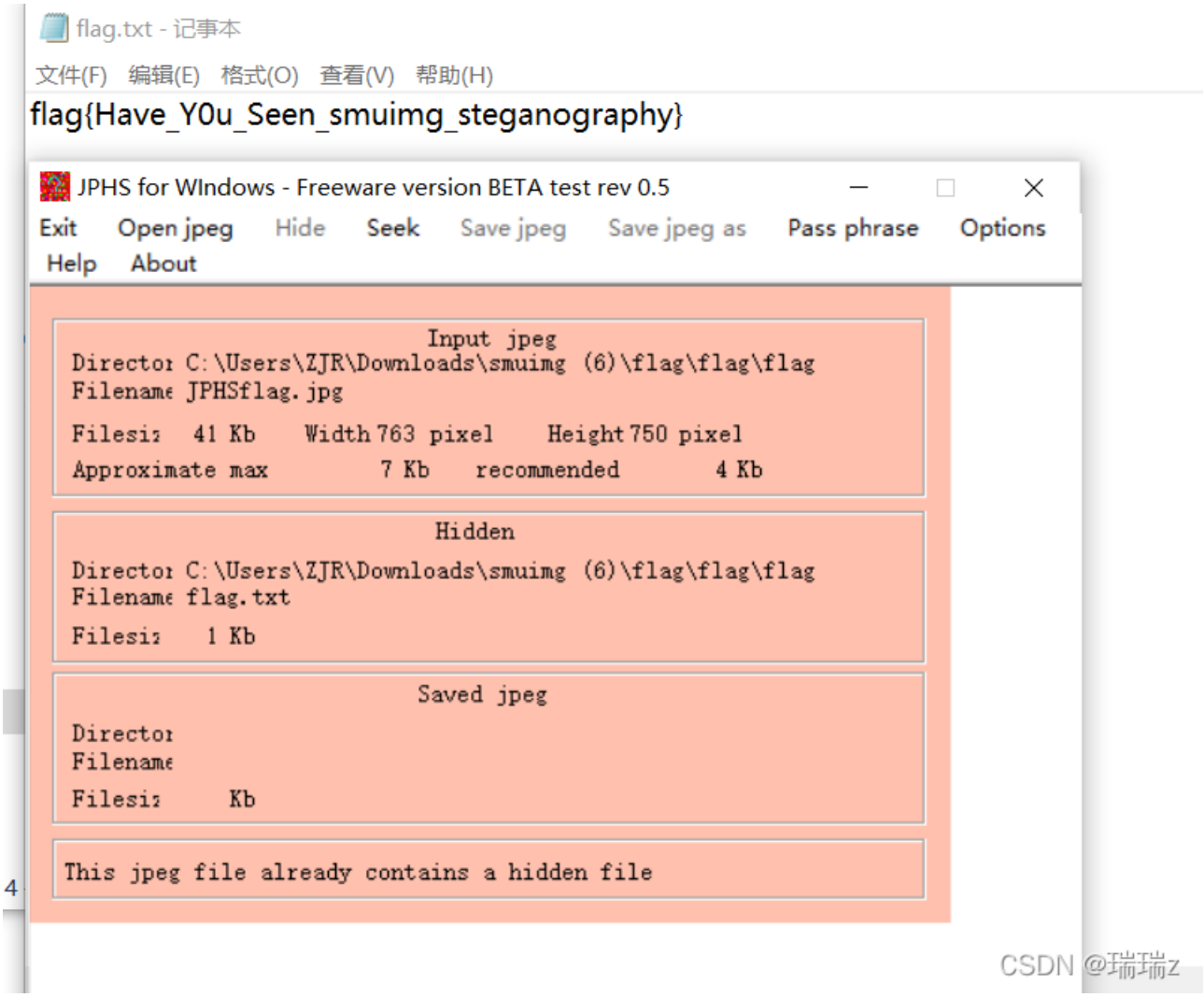
成功得到密码。

打开压缩包后里面还是一张图片和一个压缩包，这次图片的名字叫F5flag.jpg，那就用F5-steganography-master。压缩包同样的注释，所以key还是SMUCTF。



成功得到下一个密码

这一次图片叫JPHSflag.jpg,那就用Jphswin来看看。



成功得到flag！！

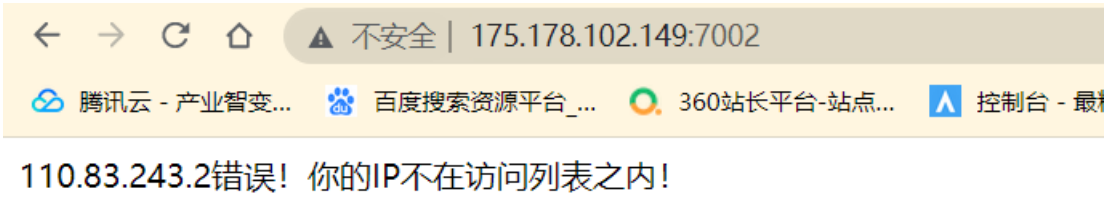
WEB

Readflag

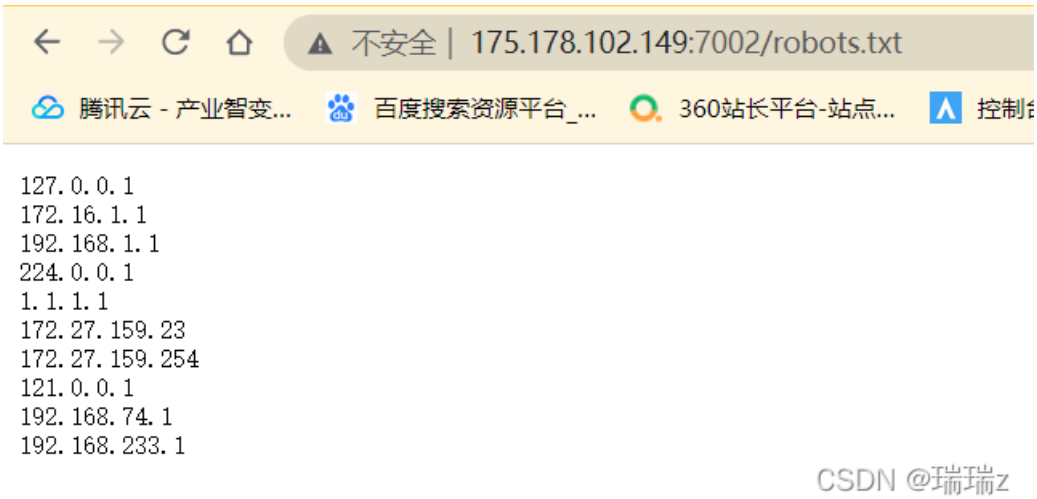
要求输入Linux命令，那首先想到flag应该是一个文件形式储存的，先 ls / 一下看看都有什么

直接 cat /flag 看看内容，即可得到flag。

XFF



查一下robots.txt

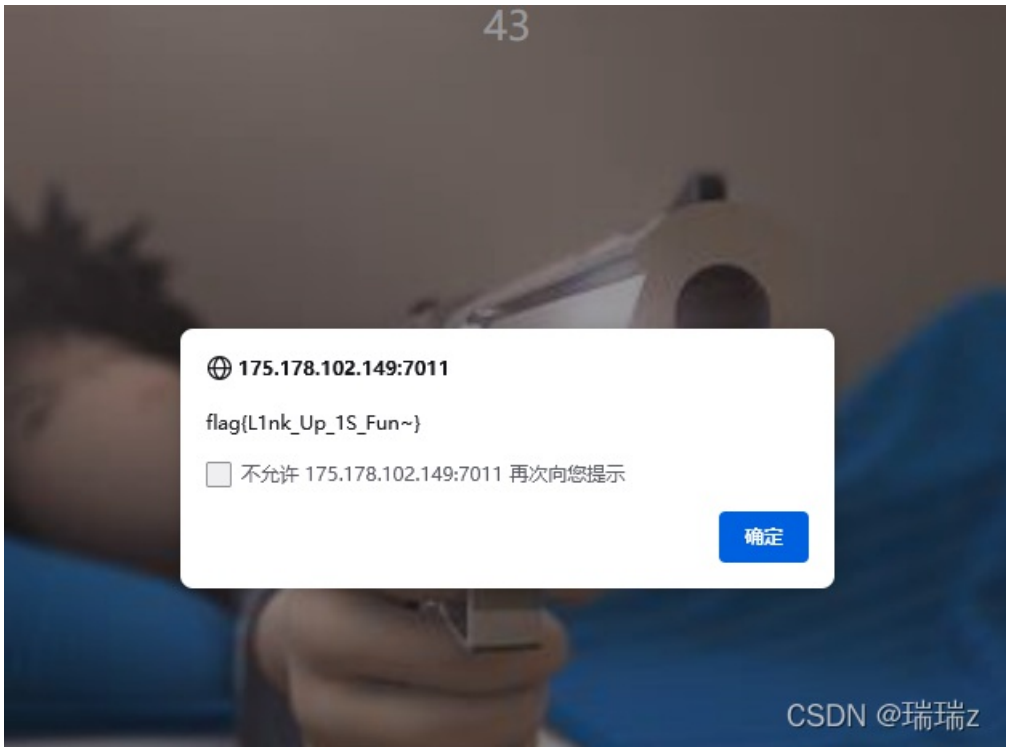


打开burp抓包，伪造ip为1.1.1.1，成功得到flag。

linkup

出题人说这是一道游戏题，那不如直接把这个简单的连连看玩通关试试。试了几次都没完成，45秒倒计时太快了。打开burp抓包，不允许数据包返回服务器，这次随便倒计时都不怕了。

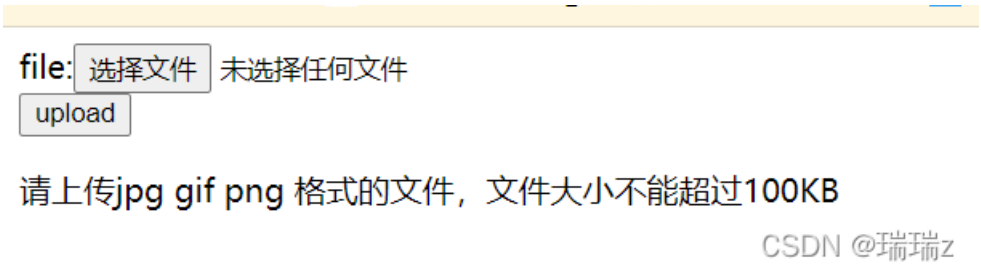
游戏通关，成功得到flag



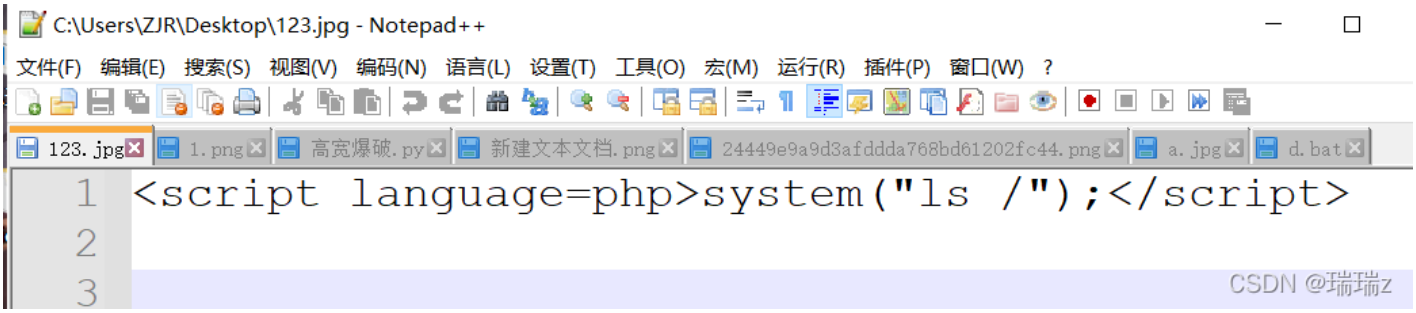
Hello

打开链接，只有一句WELCOME来欢迎我，查看一下源码，发现还有一个upload.php。

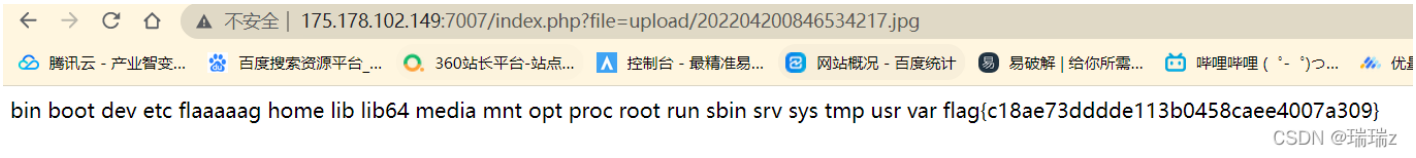
打开upload页面



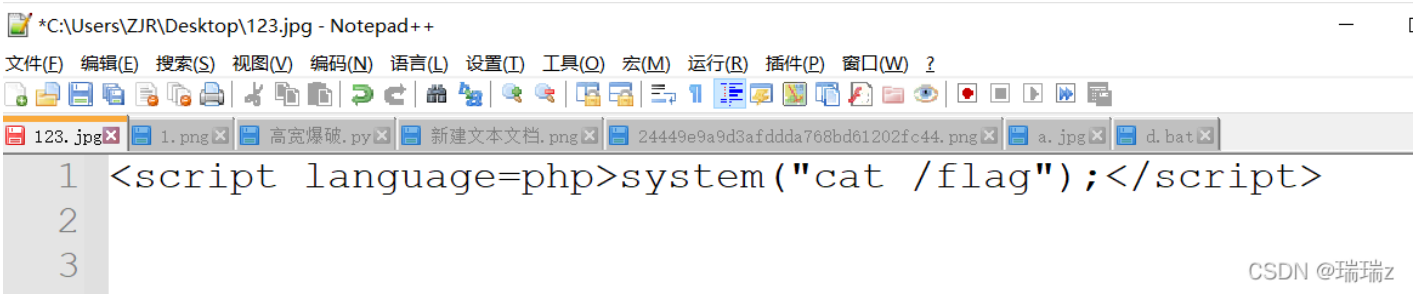
先来个一句话木马，伪装成jpg，看看目录下都有什么文件。



进入返回的保存路径



直接一句话cat一下flaaaaag，得到flag



REVERSE

合金弹头

> 由GameMaker制作，W/A/S/D控制方向，U/I开火

又是一道游戏题，玩了几关还挺有意思。

这个题关键词之处就在于GameMaker。先用gm8decompiler解包得到 .gmk文件，再用gamemaker打开，在背景图中找到flag。

```
.\gm8decompiler.exe "hjdt.exe"
```