




# SWPU新生赛2021 Misc部分WriteUp

原创

是Mumuzi  于 2021-10-11 18:14:52 发布  554  收藏 2

分类专栏: [ctf NSSCTF](#) 文章标签: [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/120582014](https://blog.csdn.net/qq_42880719/article/details/120582014)

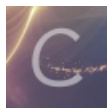
版权



[ctf](#) 同时被 2 个专栏收录

75 篇文章 28 订阅

订阅专栏



[NSSCTF](#)

6 篇文章 1 订阅

订阅专栏

## 第一波放题

你喜欢osu吗?

打开铺面发现都是重复的操作，于是看铺面文件  
发现这里的变化可能对的上二进制

```
224,224,0,5,0,0:0:0:0:
224,160,500,1,8,0:0:0:0:
224,160,1000,1,8,0:0:0:0:
224,160,1500,1,8,0:0:0:0:
224,160,2000,1,8,0:0:0:0:
224,224,2500,1,0,0:0:0:0:
224,160,3000,5,8,0:0:0:0:
224,160,3500,1,8,0:0:0:0:
224,224,4000,1,0,0:0:0:0:
224,224,4500,1,0,0:0:0:0:
224,160,5000,1,8,0:0:0:0:
224,224,5500,1,0,0:0:0:0:
224,224,6000,5,0,0:0:0:0:
224,224,6500,1,0,0:0:0:0:
224,224,7000,1,0,0:0:0:0:
224,160,7500,1,8,0:0:0:0:
224,224,8000,1,0,0:0:0:0:
224,160,8500,1,8,0:0:0:0:
224,160,9000,5,8,0:0:0:0:
224,160,9500,1,8,0:0:0:0:
224,224,10000,1,0,0:0:0:0:
224,160,10500,1,8,0:0:0:0:
224,224,11000,1,0,0:0:0:0:
224,160,11500,1,8,0:0:0:0:
224,224,12000,5,0,0:0:0:0:
224,160,12500,1,8,0:0:0:0:
224,160,13000,1,8,0:0:0:0:
224,160,13500,1,8,0:0:0:0:
224,224,14000,1,0,0:0:0:0:
224,224,14500,1,0,0:0:0:0:
224,160,15000,5,8,0:0:0:0:
224,160,15500,1,8,0:0:0:0:
224,224,16000,1,0,0:0:0:0:
```

正好和上次节奏医生的题也对的上，于是将第一行改成这玩意，跑一下写好的脚本  
发现确实是flag，再reverse一下就可以了

```
f = open('Richard Schrieber - Miracle of Life (WDLJT) [Easy].osu', 'r').readlines()
flag = ''
for i in f:
    tmp = i.split(',')
    if(tmp[4] == '0'):
        flag += '0'
    else:
        flag += '1'
print(flag)
s = ''
rflag = ''
for i in flag:
    s+=i
    if len(s)==8:
        rflag += chr(int(s,2))
        s=''
print(rflag)
print(rflag[::-1])
```

NSSCTF{i\_know\_you\_like\_osu!}

## 我的银行卡密码

我傻了，我傻了5天。

首先还是用爆破软件把密码爆出来，银行卡密码6位数字，爆破得到密码

768521

然后是一个pwd.md，我搞了5天死活忘了手机的9键，晚上做的时候突然把hint一删然后一看突然就想起来了，...

懒得一个个打下来，用脚本

```
c = '93 53 63 71 51 63 41 51 83 63 23 23 93 62 61 94 93 71 41 92 41 71 63 41 51 31 83 43 41 21 81 22 21 74 42'
table = ['ABC', 'DEF', 'GHI', 'JKL', 'MNO', 'PQRS', 'TUV', 'WXYZ']
c = c.split(' ')
for i in range(len(c)):
    print(table[int(c[i][0])-2][int(c[i][1])-1],end='')
```

得到YLOPJOGJVOC CYNMZYPGXGPOGJDVIGATBASH

atbash，将YLOPJOGJVOC CYNMZYPGXGPOGJDVIG进行atbash

得到BOLKQLTQELXXBMNABKTCTKLTQWERT

qwert密码，百度随便找个在线或者用脚本的就可以，对BOLKQLTQELXXBMNABKTCTKLT进行解密，得到

XISRASEACSUUXZYKXREVERSE

REVERSE，于是对XISRASEACSUUXZYKX进行reverse

```
print('XISRASEACSUUXZYKX'[::-1])
```

得到XKYZXUUSCAESARSIX

CAESARSIX，凯撒，6。得到RESTROOM

最后reverse

得到MOORTSER

小写提交

NSSCTF{moortser}

## here\_is\_a\_bug

解压出来D盾一扫即可

在member/zp.php里

NSSCTF{oh\_you\_catch\_the\_bug}

## 原来你也玩原神

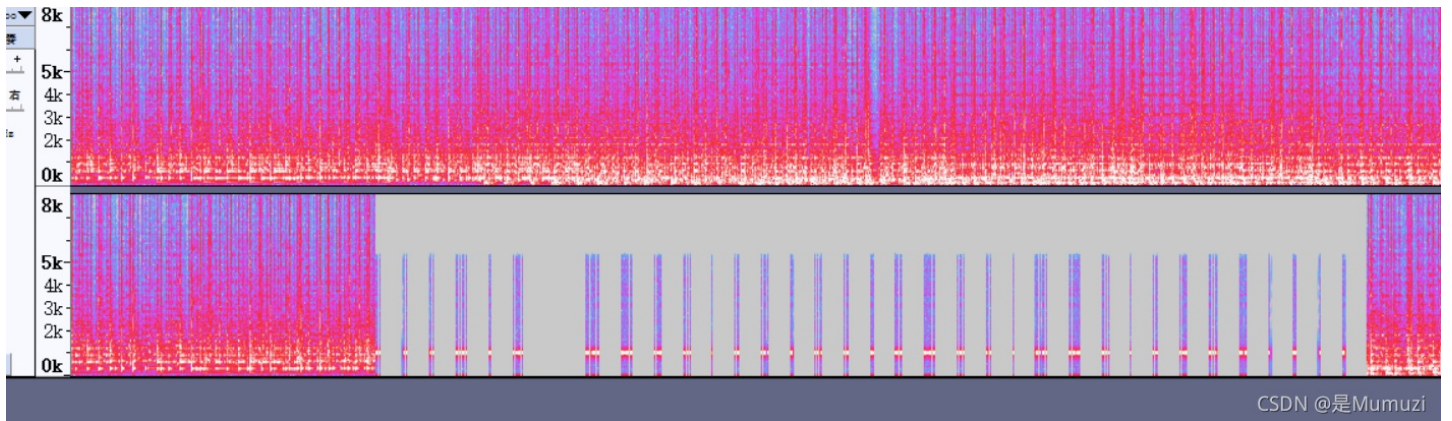
百度一下FFFB92，可知是mp3文件，改成mp3，用AU打开，查看频谱也没发现异常，于是再去用mp3stego，密码为空，得到一个txt，打开是PK开头，于是将txt改成zip，发现有伪加密，于是又将09改成00打开就是flag

NSSCTF{So\_you\_also\_play\_Genshin\_impact}

Mooooooooooooorse

又是原神

先试了下slienteye，发现不是，再去看频谱发现摩斯密码，转一下再小写就是flag



没记flag，懒得再转了，自己转

## Bill

xlsx，但是打开显示要密码，010看一下发现被分成了两部分，将504B0304前面的删掉或者直接binwalk or foremost得到xlsx

后面就老考点了，hackergame考过，之前DAS又考过

去下载一个拓展包

<http://www.ffcell.com/data/wk/201858/0217582893.html>

然后用office打开，将①全替换成壹，②全替换成贰，三替换成叁，4替换成肆，然后在

C列使用函数=ZhMoneyToNum(A1)，向下拉

D列使用=B1&"元"，向下拉

E列=ZhMoneyToNum(D1)

F列=C1\*E1

最后SUM一下就好了

```
NSSCTF{5030782.26}
```

## zipbomb

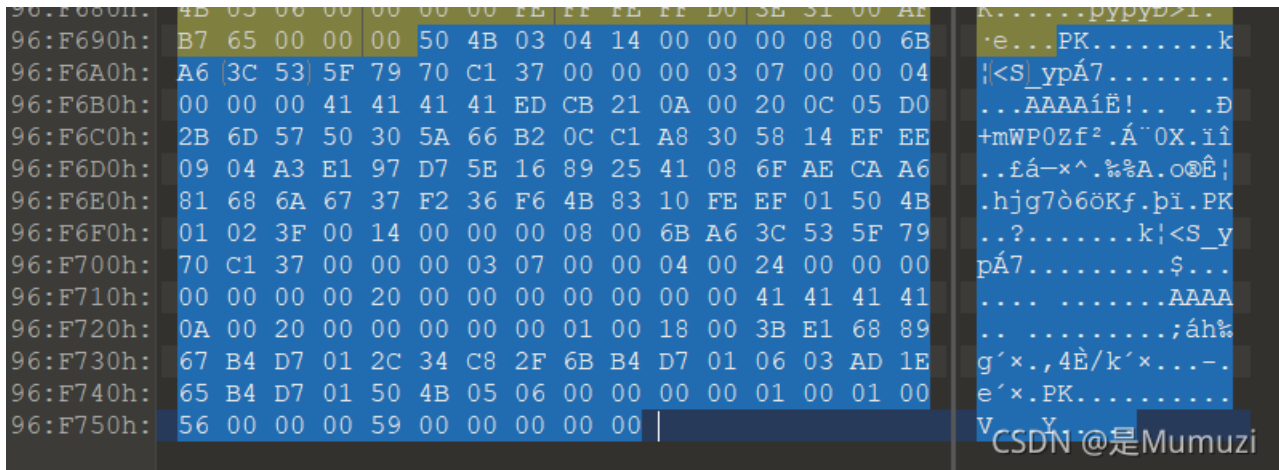
怎么又是这个考点，直接用脚本

```
import os.path
import zipfile
import re

dir_path='C:\\Users\\mumuzi\\Desktop\\NSS附件包\\MISC'
files= os.listdir(dir_path)
newfiles = ["zipbomb.zip"]
print(newfiles)
setee = []
for file in newfiles: #遍历文件夹
    position = dir_path+'\\'+ file #构造绝对路径，"\\", 其中一个\'为转义符
    print (position)
    z = zipfile.ZipFile(position, 'r')
    for filename in z.namelist():
        bytes = z.read(filename)
        if b'NSSCTF{' in bytes:
            print(filename)
```

发现在AAAA，但是整个文件夹都没有AAAA。

于是查看16进制，发现AAAA在文件尾



手动删掉前面的，完事，解压AAAA即可

```
NSSCTF{Z1p_B00m_d1sp0sal}
```

## gif好像有点大

直接打开GIFFrame

按下箭头快速翻阅，当然导出也行

找到第561帧有一个二维码，扫描即为flag



然后题目描述把NSS改成NSSCTF

```
NSSCTF{The_G1F_Is_T00_b1g}
```

## 第二波放题

## 二维码不止有二维码

这个题，，，就是很多二维码套起来的。目的是为了拓展眼见，具体哪些扫了哪些码我也忘了，还有印象的应该是code128、QR code、Maxicode、Aztec code、PDF417、汉信码等。总之，用中国编码和<https://demo.dynamsoft.com/barcode-reader/>轮着试就行。

然后code128部分，扫出来是<https://wdljt-img.oss-cn-shanghai.aliyuncs.com/NSSCTF/Barcode/dcbeba58-b686-4878-87b8-f4fa46640a34.png>

最后的flag是：

```
NSSCTF{87b87009-8f12-415b-95ee-375b28c522b7}
```

## 我flag呢？

词频分析，但是只词频{}里面的内容，而且全小写。

我弄的稍微麻烦一点

我是先用notepad++在每个'}后面加上一个换行符

即用查找模式用拓展，然后}替换为}\n

然后写脚本

```
from collections import Counter
c = ''
f = open('我flag呢? ', 'r').readlines()
for i in range(len(f)):
    ind = f[i].find('{')
    c += f[i][ind+1:-2]
f = Counter(c.lower())
f = f.most_common()
print(f)
for i in range(len(f)):
    print(f[i][0], end='')
```

输出yourflagis81e57d2bc90364t

因为t只输出了一次，应该要被舍弃，所以最后flag为

```
NSSCTF{81e57d2bc90364}
```

## Minecraft Wiki的那些事

先找到人，最开头我搜到了ff98sha还以为是大佬自出自收，后来想想应该不是，但是Ff98sha师傅也是个大牛

先找到人是WDLJT，具体方法为在Minecraft中文Wiki的微博里直接搜



然后成功发现：

Minecraft中文Wiki

2018-11-26

来自 微博 weibo.com

【公告】恭喜新巡查员WDLJT上任。

再在google搜WDLJT，找到博客<https://i.wd-jt.com/>

那里有个微博链接，点过去，再翻2018年11月的微博



The screenshot shows a Weibo post from user '问谛居' (Wendiju) dated 2018-11-27, mentioning '小米6' (Xiaomi 6) and '拍人更美' (taking photos of people is more beautiful). Below it is a reply from '@Minecraft中文Wiki' (Minecraft Chinese Wiki) dated 2018-11-26, with the text: '【公告】恭喜新巡查员WDLJT上任。' (Announcement: Congratulations to the new moderator WDLJT). The post has 2 shares, 2 comments, and 20 likes. Below the post is a comment input field with the placeholder '发布你的评论' (Post your comment) and a '评论' (Comment) button. There are also options for '同时转发' (Share at the same time) and '按热度' (Sort by popularity) / '按时间' (Sort by time). Below the comment section are two replies. The first reply is from 'Minecraft中文Wiki:原来是你' (Minecraft Chinese Wiki: It's you) dated 2018-11-28 07:23, with a sub-reply from '问谛居' (Wendiju) dated 2018-11-28 12:59. The second reply is from '问谛居' (Wendiju) dated 6-30 21:49, with the text 'AFF{Jrypbzr\_gb\_Zvarpensg}' highlighted in a red box. At the bottom right of the screenshot, there is a watermark 'CSDN @是Murnuzi'.

AFF-NSS

所以选择凯撒一下，得到flag

```
NSSCTF{Welcome_to_Minecraft}
```

## Minecraft的那些事

直接搜题目描述“曾经Mojang在Minecraft中加入了二维码”

<https://minecraft.fandom.com/wiki/彩蛋>

### 彩蛋

在超平坦世界中还会生成由覆雪构成的**二维码**，内容为“1.9 The Combat ... 这种特性在Minecraft 1.4.2中为了2012年的万圣节而加入，并在之后每年的万圣节均会出现。

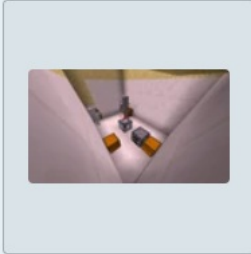
然后进去搜二维码，继续跟进到15w14a

<https://minecraft.fandom.com/zh/wiki/15w14a>



## 超平坦

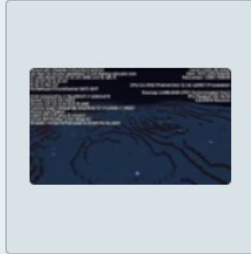
- 在超平坦世界，接近坐标 $X=0$ ,  $Z=0$ 的地方，下雨的时候会生成一个巨大的，由雪构成的二维码。扫描这个二维码会显示下一个更新的名称。
  - 有一个苦力怕的头像隐藏在二维码的左上角。



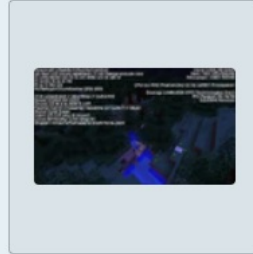
一个被变成屋子的地牢。



在森林生物群系里的一格雪。



大多数的雪融化了的冰原。



大多数的雪融化了的冷针叶林。



在地图中隐藏的二维码。



从之前的截图中提取出来的二维码，图片被重新着色。

CSDN @是Murnuzi

扫码得到flag

```
NSSCTF{Minecraft 1.9: The Combat Update}
```

## 问卷调查

回答问题即可，得到NSSCTF{NTBjYjE0ODgtNjY2Zi00OGVjLTiINGEtZWQ4ZjJiYjg0YTM0}

内容base64解码

```
NSSCTF{50cb1488-666f-48ec-9b4a-ed8f2bb84a34}
```