

攻防世界 Misc高手进阶区 4分题 Miscellaneous-300

原创

思源湖的鱼  于 2020-12-03 13:36:00 发布  472  收藏 1

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [misc](#)

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/weixin_44604541/article/details/110527034

版权

CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Misc高手进阶区的4分题

本篇是Miscellaneous-300的writeup

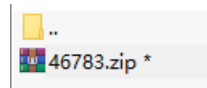
发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

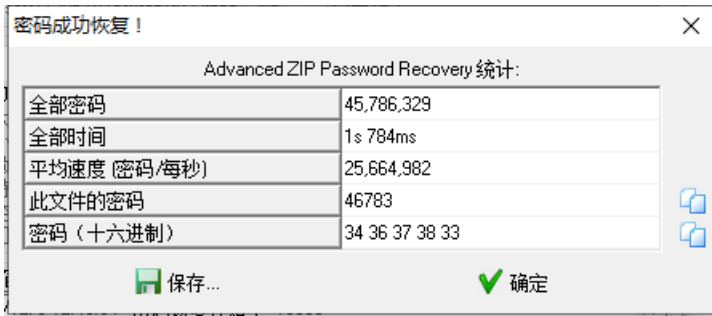
下下来一个压缩包

解压要密码



看了看不是伪加密

爆破



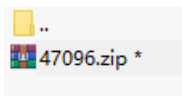
发现密码就是压缩包内文件名

解压

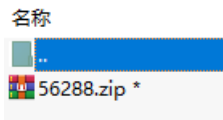
里面又是压缩包

...

难不成要套娃？



...



好的

套娃了

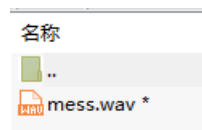
根据提示

题目描述: [\[检查这个\]\(73168.zip\)](#)

写个脚本

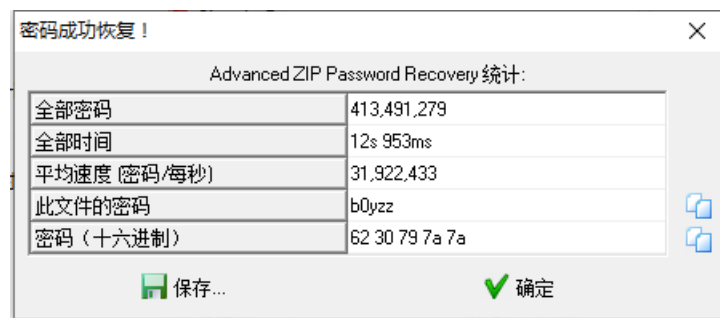
```
import zipfile
import re
zipname = "C:\\Users\\13957\\Desktop\\"+"47096.zip"
while True:
    if zipname != "C:\\Users\\13957\\Desktop\\73168.zip":
        ts1 = zipfile.ZipFile(zipname)
        res = re.search('[0-9]*', ts1.namelist()[0])
        print(res.group())
        passwd = res.group()
        ts1.extractall("C:\\Users\\13957\\Desktop\\", pwd=passwd.encode('ascii'))
        zipname = "C:\\Users\\13957\\Desktop\\"+ts1.namelist()[0]
    else:
        print("find")
```

等了好一会儿（也就1000多个包吧）
到12475.zip报错



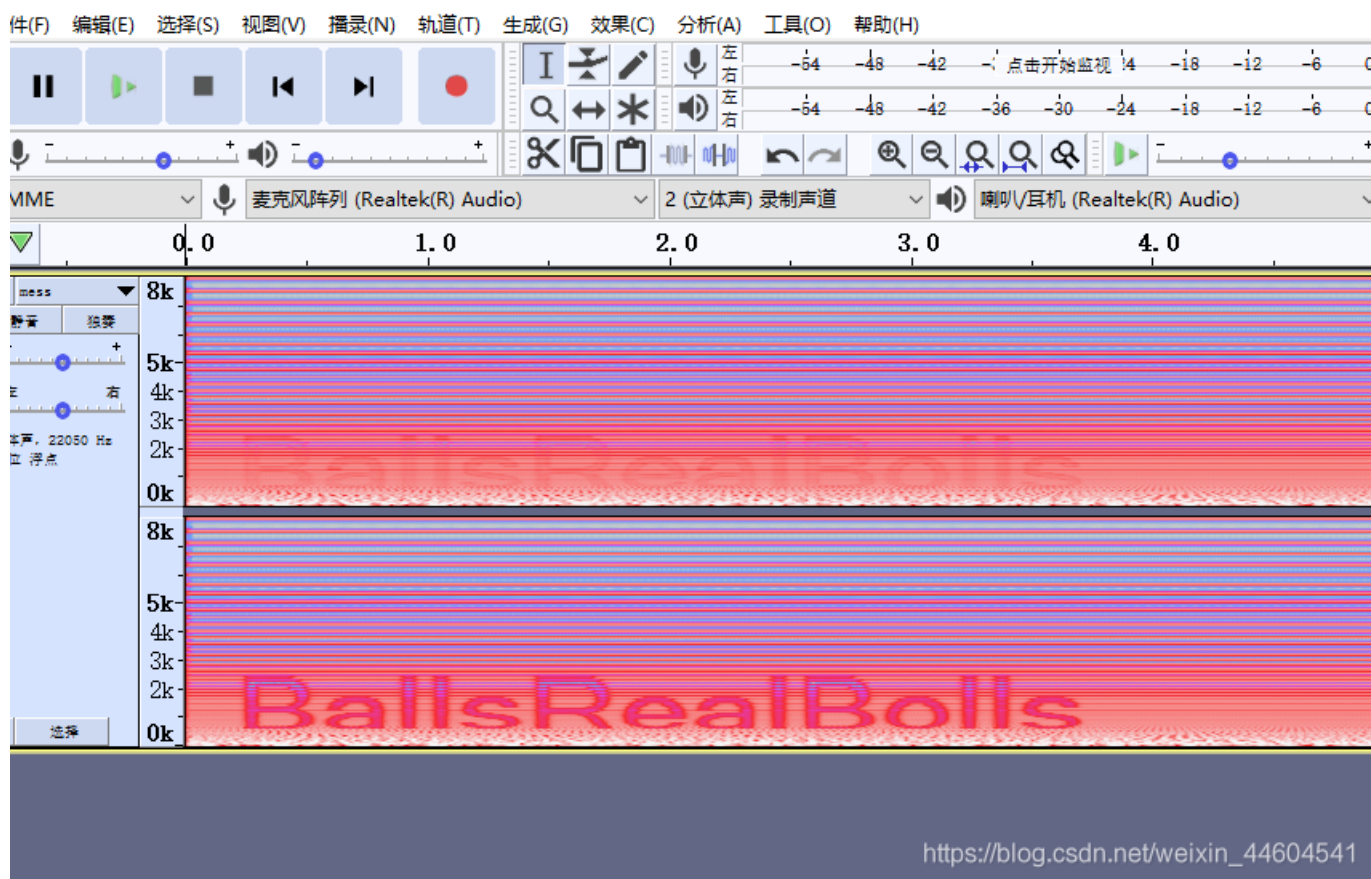
又有加密

爆破



扔进audacity

频谱图



得到flag

结语

这个套娃有点蛋疼