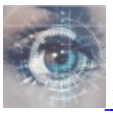
xctf攻防世界 MISC高手进阶区 Miscellaneous-300

原创

l8947943 已于 2022-01-26 00:01:50 修改 10871 收藏

分类专栏： 攻防世界misc之路 文章标签： 安全 web安全 misc

于 2022-01-26 00:01:20 首次发布

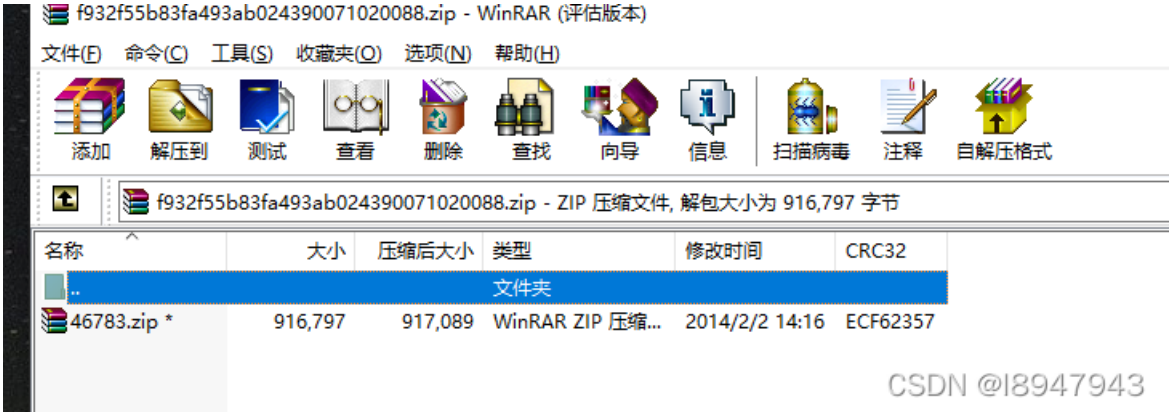


1. 进入环境，下载附件

题目给的是一个zip文件，但是带有密码，尝试放入winhex中，发现并不是伪加密。

2. 问题分析

没有提示，没有伪加密，但是打开压缩包如图：

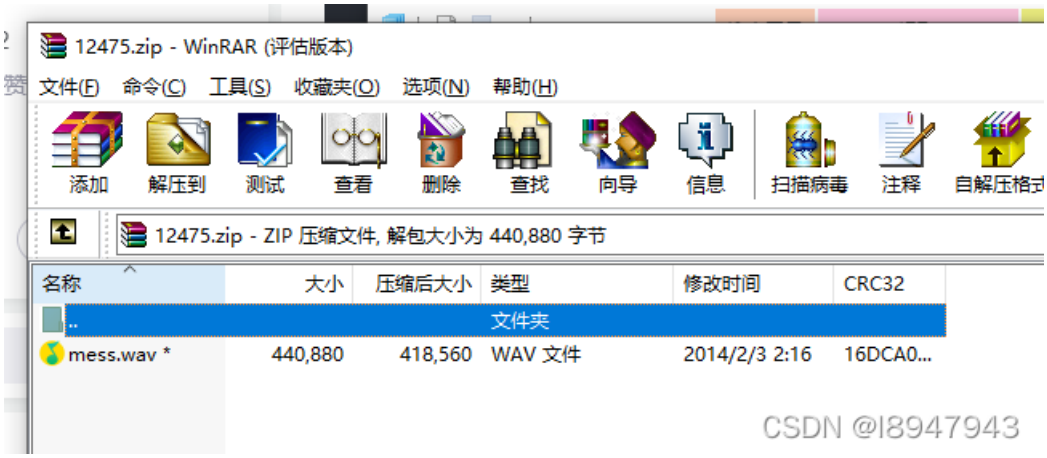


发现压缩包还有压缩包，名字数字很奇怪，尝试用它作为解压密码。竟然还成功了，反复尝试几次，才知道是俄罗斯套娃。下一个文件的解压码是里面的压缩包名。找到规律后，参考网上的wp，开始尝试代码：

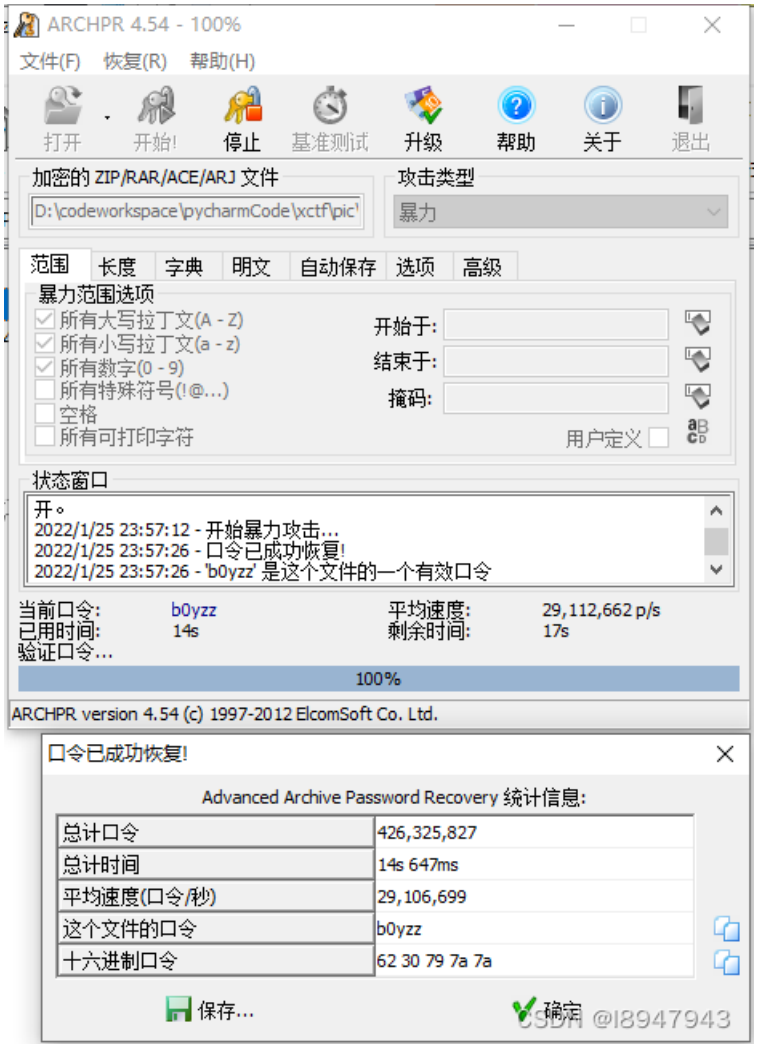
```
import zipfile
import re

file_name = 'pic/' + 'f932f55b83fa493ab024390071020088.zip'
while True:
    try:
        zf = zipfile.ZipFile(file_name)
        re_result = re.search('[0-9]*', zf.namelist()[0])
        passwd = re_result.group()
        zf.extractall(path='pic/', pwd=re_result.group().encode('ascii'))
        file_name = 'pic/' + zf.namelist()[0]
    except:
        print("get the result")
```

最后一个压缩包是22475，打开如图：



包含一个音频文件，尝试再次解压，不行，只能爆破了，掏出ARCHPR：



口令为：b0yzz

解压后，估计是音频隐写，扔到Audacity，尝试转换成频谱图：

哇靠，结果出来啦！！！最终答案为：`BallsRealBolls`