XCTF进阶区Crypto之你猜猜 write up

原创

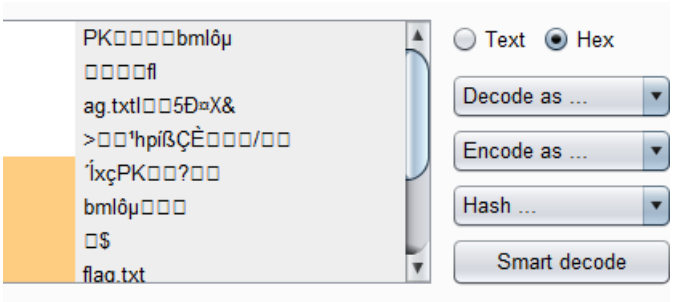
KogRow 于 2020-07-02 16:18:41 发布 1270 收藏 3
分类专栏： Crypto CTF 杂项 文章标签： misc crypto

我们刚刚拦截了，敌军的文件传输获取一份机密文件，请君速速破解。

下载下来是个txt,里面一串神秘代码：

```
504B03040A0001080000626D0A49F4B5091F1E0000001200000000800000066C61672E7478746C9F170D35D0A45826A03E161FB9687
```

猜想是十六进制数，拿去decode一下：



decode出来发现是乱码，但是内含flag.txt字样，结合开头504B0304，猜测这是一个zip的二进制数据。

因此在winHex中新建一个zip文件，解压时需要密码。

此时判断该zip是真加密还是假加密：

1.压缩源文件目录区的标记第二位是奇数：01 08

```
3F 00 0A 00 01 08 00 00
1E 00 00 00 12 00 00 00
00 00 20 00 00 00 00 00
78 74 0A 00 20 00 00 00
```

2.压缩源文件数据区标记第二位是奇数：01 08

```
50 4B 03 04 0A 00 01 08
09 1F 1E 00 00 00 12 00
61 67 2E 74 78 74 6C 9F
3E 16 1F B9 68 70 ED DF
```

尝试将其修改为偶数失败，真加密实锤了。

目前想到的办法就是爆破。

写一个python3脚本，跑字典：

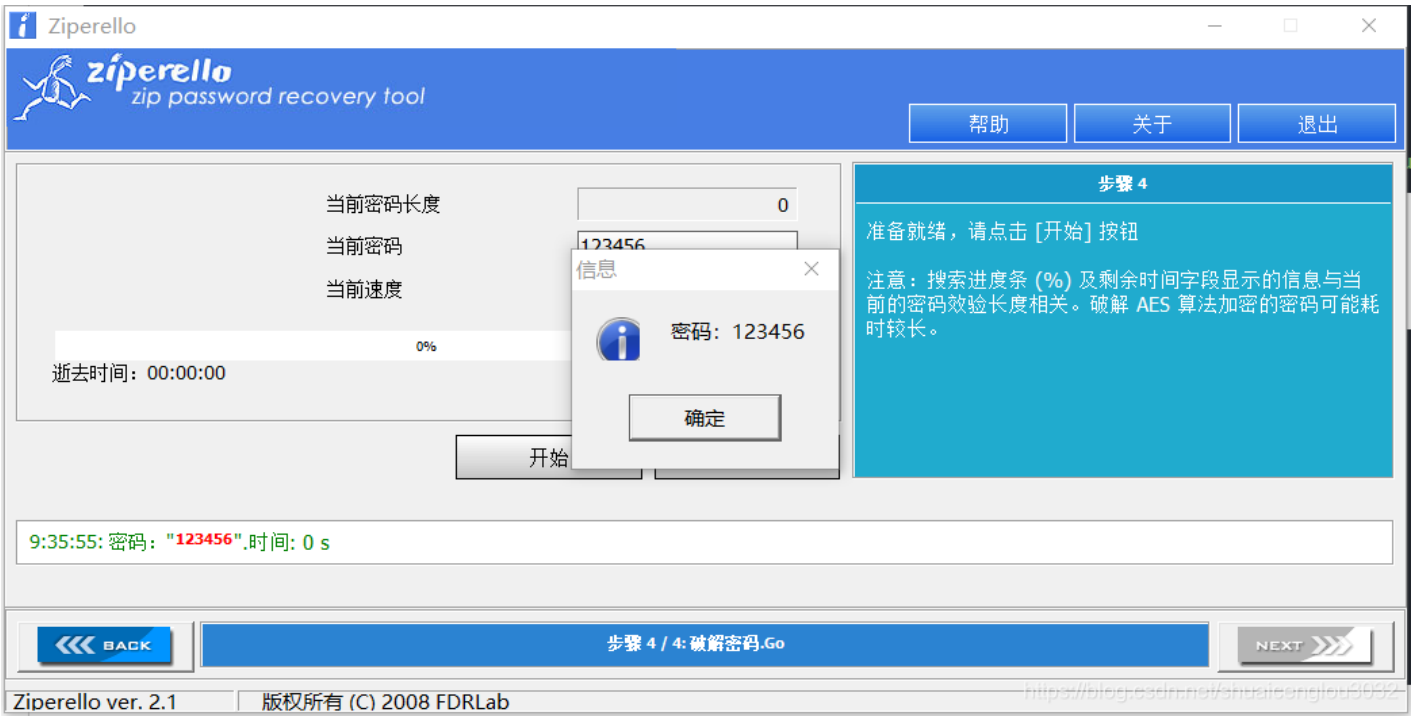
```
import zipfile #导入模块，它是做压缩和解压缩的
pwds = '1234567890'
passFile=open('E:\\informationSecurity\\pwd.txt')
i=0
zfile = zipfile.ZipFile("C:\\Users\\llllll\\Desktop\\a.zip") #要解压缩的压缩包
for line in passFile.readlines():
    pwds.append(line.replace('\n',''))
    i += 1

for j in range(0,len(pwds)):
    password=pwds[j] #我们设定的口令
    zfile.extractall(path='C:\\Users\\llll\\Desktop', members=zfile.namelist(), pwd="123456".encode('utf-8'
```

但是读取字典会报错，直接在代码里声明密码时就不会，原因不明。

```
Traceback (most recent call last):
    File "E:/05.Project/01.Python/Aziji-usefully/force_unlock_zipfile/d.py", line 10, in <module>
      fn.extractall(pwd=b'100100')
   File "C:\Program Files\Python37\lib\zipfile.py", line 1594, in extractall
     self._extract_member(zipinfo, path, pwd)
   File "C:\Program Files\Python37\lib\zipfile.py", line 1647, in _extract_member
     with self.open(member, pwd=pwd) as source, \
   File "C:\Program Files\Python37\lib\zipfile.py", line 1516, in open
     raise RuntimeError("Bad password for file %r" % name)
```

所以不用代码了，使用工具Ziperello爆破：



最后跑出来密码是123456.

解压成功拿到flag: