套娃

发表于 2021-01-15 分类于 Challenge， 2020， 安洵杯， Misc
Challenge | 2020 | 安洵杯 | Misc | 套娃

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/8581

题目考点

- *crc32*
- *zip刁钻爆破姿势*

解题思路

crc32爆破得到解压密码`!qQIdEa@#!z)`

解压得到easyzip.zip

然后用7z打开easyzip.zip，得到明文readme.txt

然后备份easyzip.zip,之后用winrar把readme.txt和flag.txt删除，留下readme.txt副本，然后已知明文攻击

已知明文攻击得到密码`%3#c$v!@`

然后用这个密码解密原来easyzip.zip中的flag.txt

*最后解base64*3和栅栏3*

贴上crc32爆破脚本

```
import binascii

for i in range(32,127):
    for j in range(32,127):
    #print(chr(i))
        crc = binascii.crc32(chr(i)+chr(j)) & 0xffffffff
        crc_f = ['EA4446B6','ED7987DE','46FE0943','4BE30989','B31975C0','D6BB1BEF']
        find = hex(crc).upper()[2:]
        #print(find)
        if find in crc_f:
            print(chr(i)+chr(j)+"   "+find)
```

Flag

```
flag{zip&crc_we_can_do_it}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/安洵杯/Misc/p4cCR9zsi8jXrMQU2aNzzt.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # Misc # 安洵杯
王牌特工
签到