CTF-Misc-Rar文件中的crc碰撞

原创

SuperGate 于 2019-06-09 14:36:48 发布 3184 收藏 7
分类专栏： CTF-MISC

Misc中的有一类题目是要求我们知道加密后的rar文件中的内容。但是rar文件密码我们不知道，直接爆破密码也不是很现实。

但是当文件的大小比较小，或者字符数量较少时，就可以根据crc校验码来爆破出rar内部文件的内容。

..			文件夹		
flag_0.txt *	4	16	文本文档	2018/9/22 23:...	7DE0AB32
flag_1.txt *	4	16	文本文档	2018/9/22 23:...	B1441D53
flag_2.txt *	4	16	文本文档	2018/9/22 23:...	49BD11F5
flag_3.txt *	4	16	文本文档	2018/9/22 23:...	B42F1DFA
flag_4.txt *	4	16	文本文档	2018/9/22 23:...	8163F43E
flag_5.txt *	4	16	文本文档	2018/9/22 23:...	1FC8FEE5
another_flag.txt *	22	36	文本文档	2018/9/22 23:...	A9E6A804
flag.txt *	30	44	文本文档	2018/9/22 23:...	E6F2C401

这种类型的rar，flag由flag_0~flag_5组成。rar文件是有密码的，无法直接打开这些文件。

可以看到最后一列是对应文件的CRC校验码。并且每个文件只有4字节，所以可以看作每个crc校验码都对应了唯一的文件。

因此考虑CRC碰撞。

CRC碰撞原理就是构造一个和源文件等长的字符串，然后再对其进行CRC校验，比较校验码是否相同即可。

```
import binascii
import string

dic=string.printable #打印出字符表
crc1=0x7DE0AB32
crc2=0xB1441D53
crc3=0x49BD11F5
crc4=0xB42F1DFA
crc5=0x8163F43E
crc6=0x1FC8FEE5

for i in dic:
    for j in dic:
        for n in dic:
            for m in dic:
                s=i+j+n+m
                if(crc1==(binascii.crc32(s) & 0xffffffff)):
                    text1=s
                if (crc2 == (binascii.crc32(s) & 0xffffffff)):
                    text2=s
                if (crc3 == (binascii.crc32(s) & 0xffffffff)):
                    text3=s
                if (crc4 == (binascii.crc32(s) & 0xffffffff)):
                    text4=s
                if (crc5 == (binascii.crc32(s) & 0xffffffff)):
                    text5=s
                if (crc6 == (binascii.crc32(s) & 0xffffffff)):
                    text6=s
print text1+text2+text3+text4+text5+text6
```