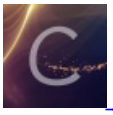
ISC 2018 蓝鲸魔塔线上赛Reverse题目PYMD5 Writeup

原创

iqiqiya 于 2018-10-28 17:21:15 发布 460 收藏 1
分类专栏： 我的逆向之路 我的CTF之路 ------python学习 我的CTF进阶之路 文章标签： ISC 2018 蓝鲸魔塔线上赛Reverse题目PYMD5 Reverse题目PYMD5 Writeup ISC 2018 蓝鲸魔塔线上赛Reverse Reverse

 我的逆向之路 同时被 3 个专栏收录
108 篇文章 10 订阅
订阅专栏

 我的CTF之路
92 篇文章 5 订阅
订阅专栏

 ------python学习
11 篇文章 0 订阅
订阅专栏

找到了一道pyc逆向题目

拿来玩玩

下载得到一个压缩包 解压后拿到PYMD5.pyc

notepad++打开是乱码

ubuntu装上uncompyle

```
iqiqiya@521:~/Desktop$ uncompyle6 PYMD5.pyc > pymd5.py
```

处理一下拿到py文件　内容如下：

```
# uncompyle6 version 3.2.4
# Python bytecode 2.7 (62211)
# Decompiled from: Python 2.7.6 (default, Nov 23 2017, 15:49:48)
# [GCC 4.8.4]
# Embedded file name: unVm.py
# Compiled at: 2018-04-17 01:42:14
import md5
md5s = [408729002343402003523114968491717869 25L,
 377748712743872269115446269098532971 47L,
 136364329640288194110852557127415197202L,
 197102543045186090881257886713375686009L,
 462827909716099265741813648792322457 14L,
 199788626591470902691740865303843697496L,
 139155483798021197733301619201494834453L,
 105977393849615850942572250680575701536L,
 103383262965894787541607484291344857033L,
 193549894376121578282270539756256252317L]
print 'Can you turn me back to python ? ...'
flag = raw_input('well as you wish.. what is the flag: ')
if len(flag) > 50:                #flag总长度小于等于50
    print 'nice try'
    exit()
if len(flag) % 5 != 0:            #flag长度是5的倍数
    print 'nice try'
    exit()
for i in range(0, len(flag), 5):  #每次取5位赋值给s 进行md5(s)生成十六进制的串 再转十进制与md5s进行比较
    s = flag[i:i + 5]
    if int('0x' + md5.new(s).hexdigest(), 16) != md5s[i / 5]:
        print 'nice try'
        exit()

print 'Congratz now you have the flag'
# okay decompiling PYMD5.pyc
```

分析可以知道 flag应该是5*10 = 50位

根据经验 猜测每五位都是小写字母

先将md5s转成十六进制

```
md5s = [40872900234340200352311496849171786925L,
 37774871274387226911544626909853297147L,
 13636432964028819411085255712741519720 2L,
 19710254304518609088125788671337568600 9L,
 46282790971609926574181364879232245714L,
 19978862659147090269174086530384369749 6L,
 13915548379802119773330161920149483445 3L,
 10597739384961585094257225068057570153 6L,
 10338326296589478754160748429134485703 3L,
 19354989437612157828227053975625625231 7L]
for i in md5s:
    print('{:x}'.format(i))
'''得到下面
1ebfd5913ef450b92b9e65b6de09acad
1c6b2cf25eb36540376a3b3fa208a9fb
6696d088517c9390167fedb2bc876e12
944891a872a4891002f7caf24c70fd79
22d1bdc61cc009b82c178607a3569fd2
964de3cd368503d06156731676aff358
68b05f0ea56017a63e7255c991fd5d15
4fba80ed85d2b50ece2dd336da68b220
4dc6e4668713974d68d44544fa7177c9
919c5a8e20ae0da98ca1f673f7ae519d'''
```

接着这里可以md5爆破(ps:工具，脚本都可以的)

有个比较巧的办法就是直接md5在线解密

```
#这是爆破第一部分
import hashlib
dic=['a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z
for a in range(len(dic)):
    for b in range(len(dic)):
        for c in range(len(dic)):
            for d in range(len(dic)):
                for e in range(len(dic)):
                    m=dic[a]+dic[b]+dic[c]+dic[d]+dic[e]
                    flag=hashlib.md5()
                    flag.update(m)
                    md5=flag.hexdigest()
                    if md5=='1ebfd5913ef450b92b9e65b6de09acad':
                        print m
                        print md5
#whale
#1ebfd5913ef450b92b9e65b6de09acad   把这个分别替换再拼接下即可拿到flag
```

这个可以得到第一部分whale

把md5分别替换再拼接下即可拿到flag

参考链接：

https://blog.csdn.net/qq_36609913/article/details/78642078

https://www.jianshu.com/p/ff81b07d1c76