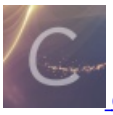
攻防世界Reverse进阶区-re4-unvm-me-writeup

原创

y4ung 于 2020-11-05 10:37:53 发布 301 收藏

分类专栏： ctf 文章标签： ctf

本文链接：https://blog.csdn.net/qq_35056292/article/details/109506556



1. 介绍

本题是xctf攻防世界中Reverse的进阶区的题re4-unvm-me

题目来源： alexctf-2017

2. 分析

文件是一个pyc文件，将该文件上传到pyc反编译网站中，得到源代码：

```
# uncompyle6 version 3.5.0
# Python bytecode 2.7 (62211)
# Decompiled from: Python 2.7.5 (default, Aug  7 2019, 00:51:29)
# [GCC 4.8.5 20150623 (Red Hat 4.8.5-39)]
# Embedded file name: unvm_me.py
# Compiled at: 2016-12-21 05:44:01
import md5
md5s = [
 174282896860968005525213562254350376167L, 137092044126081477479435678296496849608L, 126300127609096051658061491
018211963916L, 314989972419727999226545215739316729360L, 256525866025901597224592941642385934114L, 1151411388101
515712096182827284082110531, 870597347094265257792933693938390615821, 256697681645515528548061291580728800189L, 3
981855265217027434085114429591309159 9L, 653135619778120180462009978989043133501, 230909080238053318105407334248 2
28870753L, 196125799557195268866757688147870815374L, 748741451323455030953072766147279158851]
print 'Can you turn me back to python ? ...'
flag = raw_input('well as you wish.. what is the flag: ')
if len(flag) > 69:  # 长度不能大于69
    print 'nice try'
    exit()
if len(flag) % 5 != 0:  # 长度必须是5的倍数
    print 'nice try'
    exit()
for i in range(0, len(flag), 5):
    s = flag[i:i + 5]  # 每次取5个字符
    if int('0x' + md5.new(s).hexdigest(), 16) != md5s[(i / 5)]:
        print 'nice try'
        exit()

print 'Congratz now you have the flag'
```

程序比较简单，用户输入一个字符串flag，每次从flag中取5个字符赋值给s，并计算s的md5的摘要，然后在前面加个`0x`，转成16进制的值，再与数组md5s中的每个值进行比较。如果都相等，则输出正确的消息。

写个python脚本，把每5个字符对应的md5摘要值计算出来：

```
md5s = [174282896860968005525213562254350376167, 137092044126081477479435678296496849608, 126300127609096051658061491018211963916, 31498997241972799922654521573931672936025901597224592941642385934114, 11514113881015157120961828272840821105387059734709426525779293369938390615822566976816455155285480612915807288001893981855265217027434085114429591309159965313561977812018046200997898904313350, 23090908023805331810540733424822887075319612579955719526886675768814787081537496125457951323455030953072766147279158857487414513234550309530727661472791588]
raw_md5s = []
for each in md5s:
    hex_val = hex(each)
    raw_md5s.append(hex_val[2:])

print(raw_md5s)
```

输出为：

```
['831daa3c843ba8b087c895f0ed305ce7', '6722f7a07246c6af20662b855846c2c8', '5f04850fec81a27ab5fc98befa4eb40c', 'ecf8dcac7503e63a6a3667c5fb94f610', 'c0fd15ae2c3931bc1e140523ae934722', '569f606fd6da5d612f10cfb95c0bde6d', '68cb5a1cf54c078bf0e7e89584c1a4e', 'c11e2cd82d1f9fbd7e4d6ee9581ff3bd', '1df4c637d625313720f45706a48ff20f', '3122ef3a001aaecdb8dd9d843c029e06', 'adb778a0f729293e7e0b19b96a4c5a61', '938c747c6a051b3e163eb802a325148e', '38543c5e820dd9403b57beff6020596d']
```

将这些值放到cmd5网站和 hashes.com 这个网站比较牛逼中查询

> 需要注意的是，68cb5a1cf54c078bf0e7e89584c1a4e 少了一位，在前面手动补个0即可。

最终结果如下：

md5	原始值
831daa3c843ba8b087c895f0ed305ce7	ALEXC
6722f7a07246c6af20662b855846c2c8	TF{dv
5f04850fec81a27ab5fc98befa4eb40c	5d4s2
ecf8dcac7503e63a6a3667c5fb94f610	vj8nk
c0fd15ae2c3931bc1e140523ae934722	43s8d
569f606fd6da5d612f10cfb95c0bde6d	8l6m1
068cb5a1cf54c078bf0e7e89584c1a4e	n5l67
c11e2cd82d1f9fbd7e4d6ee9581ff3bd	ds9v4
1df4c637d625313720f45706a48ff20f	1n52n
3122ef3a001aaecdb8dd9d843c029e06	v37j4
adb778a0f729293e7e0b19b96a4c5a61	81h3d
938c747c6a051b3e163eb802a325148e	28n4b
38543c5e820dd9403b57beff6020596d	6v3k}

因此，flag为：`ALEXCTF{dv5d4s2vj8nk43s8d8l6m1n5l67ds9v41n52nv37j481h3d28n4b6v3k}`

3. 总结

遇到题目文件是pyc的文件扩展名，直接放到在线的pyc反编译网站中得到源码，再对源码去逆向分析即可。