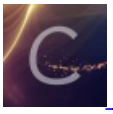
# 【jarvisoj刷题之旅】逆向题目FindKey的writeup

原创

iqiqiya 于 2018-09-10 23:39:30 发布 639 收藏
分类专栏： 我的CTF之路 我的逆向之路 我的CTF进阶之路 文章标签： 【jarvisoj刷题之旅】逆向题目FindKey的writ FindKey的writeup 逆向题目FindKey






我把下载到的文件放在了c盘根目录·

Ubuntu子系统 file一下

```
iqiqiya@DESKTOP-POI8NIV:/mnt/c$ file findkey
findkey: python 2.7 byte-compiled
iqiqiya@DESKTOP-POI8NIV:/mnt/c$
```

百度应该是.pyc文件

找到反编译工具uncompyle6

```
C:\Users\[redacted]>pip install uncompyle6
Collecting uncompyle6
  Downloading https://files.pythonhosted.org/packages/b1/81/6f51ce184aae921d770a17503ba6bc49e1ab72950bbb916e5268ea4e9b14
/uncompyle6-3.2.3-py36-none-any.whl (200kB)
    100% |████████████████████████████████| 204kB 30kB/s
Collecting xdis<3.9.0,>=3.8.4 (from uncompyle6)
  Downloading https://files.pythonhosted.org/packages/d0/f0/c48969cc5dda6989bce9e0a4f10e204eb1813b3531a5f955bfe2045ec30f
/xdis-3.8.7-py36-none-any.whl (85kB)
    100% |████████████████████████████████| 92kB 21kB/s
Collecting spark-parser<1.9.0,>=1.8.5 (from uncompyle6)
  Downloading https://files.pythonhosted.org/packages/06/13/4da9bccbef8da3c8ff6f113f69992ba34cdbe4d9fb768e25a79f8b0e304b
-/spark_parser-1.8.7-py3-none-any.whl
Requirement already satisfied: click in d:\xin\anaconda3\lib\site-packages (from spark-parser<1.9.0,>=1.8.5->uncompyle6)
 (6.7)
Installing collected packages: xdis, spark-parser, uncompyle6
Successfully installed spark-parser-1.8.7 uncompyle6-3.2.3 xdis-3.8.7
                                                    https://blog.csdn.net/xiangshangbashaonian
```

后缀加上.pyc

```
C:\>uncompyle6 findkey.pyc
# uncompyle6 version 3.2.3
# Python bytecode 2.7 (62211)
# Decompiled from: Python 3.6.5 |Anaconda custom (64-bit)| (defau
# Embedded file name: findkey
# Compiled at: 2016-04-30 17:54:18
import sys
lookup = [
 196,
 153, 149,
```



```
print 'Congratulations!!'
# okay decompiling findkey.pyc
```



反编译成功

分析一下直接改就行

```python
# Embedded file name: findkey
# Compiled at: 2016-04-30 17:54:18
import sys
lookup = [
 196,
 153, 149,
 206, 17,
 221, 10, 217, 167, 18, 36, 135, 103, 61, 111, 31, 92, 152, 21, 228, 105, 191, 173, 41, 2, 245,
    23, 144, 1, 246, 89, 178, 182, 119, 38, 85, 48, 226, 165, 241, 166, 214, 71, 90, 151, 3, 109,
    169, 150, 224, 69, 156, 158, 57, 181, 29, 200, 37, 51, 252, 227, 93, 65, 82, 66, 80, 170, 77,
    49, 177, 81, 94, 202, 107, 25, 73, 148, 98, 129, 231, 212, 14, 84, 121, 174, 171, 64, 180, 233,
    74, 140, 242, 75, 104, 253, 44, 39, 87, 86, 27, 68, 22, 55, 76, 35, 248, 96, 5, 56, 20, 161, 213,
    238, 220, 72, 100, 247, 8, 63, 249, 145, 243, 155, 222, 122, 32, 43, 186, 0, 102, 216, 126, 15,
    42, 115, 138, 240, 147, 229, 204, 117, 223, 141, 159, 131, 232, 124, 254, 60, 116, 46, 113, 79,
    16, 128, 6, 251, 40, 205, 137, 199, 83, 54, 188, 19, 184, 201, 110, 255, 26, 91, 211, 132, 160,
    168, 154, 185, 183, 244, 78, 33, 123, 28, 59, 12, 210, 218, 47, 163, 215, 209, 108, 235, 237,
    118, 101, 24, 234, 106, 143, 88, 9, 136, 95, 30, 193, 176, 225, 198, 197, 194, 239, 134, 162,
    192, 11, 70, 58, 187, 50, 67, 236, 230, 13, 99, 190, 208, 207, 7, 53, 219, 203, 62, 114, 127,
    125, 164, 179, 175, 112, 172, 250, 133, 130, 52, 189, 97, 146, 34, 157, 120, 195, 45, 4, 142, 139]
pwda = [188, 155, 11, 58, 251, 208, 204, 202, 150, 120, 206, 237, 114, 92, 126, 6, 42]
pwdb = [53, 222, 230, 35, 67, 248, 226, 216, 17, 209, 32, 2, 181, 200, 171, 60, 108]
'''flag = raw_input('Input your Key:').strip()
if len(flag) != 17:
    print 'Wrong Key!!'
    sys.exit(1)'''
flag = ''
for i in range(0, 17):
    flag += chr(lookup[i + pwdb[i]] - pwda[i] & 255)
print (flag[::-1])
      # sys.exit(1)
```

```
Run: FindKey
C:\Users\[redacted]\PycharmProjects\test\Scripts\python.exe C:/Users/[redacted]/PycharmProjects/reverse/jarvisoj/FindKey.py
PCTF{PyC_Cr4ck3r}
```



正确

FindKey 268 SOLVERS 150 REVERSE

FLAG就是你输入的key

findkey.31a509f4006ba41368dcf963762388bb

PCTF{PyC_Cr4ck3r} SUBMIT

Correct Answer!!Congratulations!