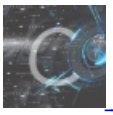
[pasecactf_2019]tornado_casino

原创

无名函数 于 2021-08-29 22:53:38 发布 184 收藏 1

分类专栏： Buu-crypto 文章标签： Buu-crypto

本文链接：https://blog.csdn.net/m0_57291352/article/details/119987361



[pasecactf_2019]tornado_casino

题目

```
from sys import argv
from random import getrandbits

flag = '<redacted>'

tornado_banner = '''
                                                        88
  ,d                                                    88
  88                                                    88
MM88MMM ,adPPYba,  8b,dPPYba, 8b,dPPYba,  ,adPPYYba,  ,adPPYb,88  ,adPPYba,
  88   a8"     "8a 88P'    "Y8 88P'   `"8a ""     `Y8 a8"    `Y88 a8"     "8a
  88   8b       d8 88         88       88 ,adPPPPP88 8b       88 8b       d8
  88,  "8a,   ,a8" 88         88       88 88,    ,88 "8a,   ,d88 "8a,   ,a8"
  "Y888 `"YbbdP"'  88         88       88 `"8bbdP"Y8  `"8bbdP"Y8  `"YbbdP"' '''
casino_banner = '''
                               88
                               ""


 ,adPPYba, ,adPPYYba, ,adPPYba, 88 8b,dPPYba,   ,adPPYba,
a8"     "" ""     `Y8 I8[    "" 88 88P\'   `"8a a8"     "8a
8b         ,adPPPPP88  `"Y8ba,  88 88       88 8b       d8
"8a,   ,aa 88,    ,88 aa    ]8I 88 88       88 "8a,   ,a8"
 `"Ybbd8"' `"8bbdP"Y8 `"YbbdP"\' 88 88       88  `"YbbdP"\' '''
tornado_art = '''

   ((  "####@@!!$$    ))
       `#####@@!$$`   ))
    ((  '####@!!$:
   ((  ,####@!!$:    ))
       .###@!!$:
       `##@@!$:
        `#@!!$
  !@#    `#@!$:       @#$
   #$     `#@!$:       !@!
            '@!$:
         ``\   "!$: /``
```

```
            \   !: /
             "\ : /"
  -."-/\\\-."//.-"/:`\."-.JrS"."-=_\\
" -."-.\\"-."//.-".`-."_\\-."-.-\".-//'''


welcome = 'Welcome!\n[1] - To slotmachine\n[2] - Enter promocode\n[3] - Exit\n'''
def sltmchn_wndw(num):
    print(num)
    return '|' + '|'.join(list(hex(num)[2:].zfill(8))) + '|'
slotmachine_menu = '[$] - $$$SPIN$$$\n'


print(tornado_banner)
print(casino_banner)
print(tornado_art)
user_balance = 10#$
promo = ''
while True:
    choice1 = input(welcome)
    if choice1 == '1':
        print('$$$Its point of no return!$$$\n$$$     all or nothing    $$$\n')
        print(f'Your balance: {user_balance}')
        while True:
            if user_balance > 0:
                spin = input(slotmachine_menu)
                if spin == '$':
                    state = getrandbits(32)
                    try:
                        pff_try = int(input('It will be: '), 16)
                    except:
                        exit(0)
                    if pff_try == state:
                        print(sltmchn_wndw(state))
                        print('OMGWTF$$$$$$$$$$$')
                        print(flag)
                        exit(0)
                    else:
                        print(sltmchn_wndw(state))
                        print('Nice try!')
                        user_balance -= 1
                        print(f'Your balance: {user_balance}')
                else:
                    exit(0)
            else:
                print('Sorry!')
                exit(0)

    elif choice1 == '2':
        if not promo:
            promo = input('Enter your promocode: ')
            if promo == 'b33_1_4m_b3333':
                print('Great!')
                user_balance += 1000#$
        else:
            print('Only once!')

    elif choice1 == '3':
        exit(0)
```

解题

先读程序：

random.getrandbits(32)来生成随机数。

random.getrandbits()使用的是MT19937（伪随机数生成）。

因此我们只要获得连续的624组随机数数据，我们就可以准确获得下一个。

代码如下：

```
from pwn import *
from mt19937predictor import MT19937Predictor

ip = '127.0.0.1'
port = '25028'
c = connect(ip, port)
print(type(c))
context.log_level = 'debug'

predictor = MT19937Predictor()

def promo(c):
    c.recvuntil("Welcome")
    c.recvline()
    c.recvline()
    c.recvline()
    c.recvline()
    c.sendline('2')
    c.recvuntil('Enter your promocode:')
    c.sendline("b33_1_4m_b3333")
    print(c.recvline())

result = []

def attack(c):
    c.sendline("1")
    c.recvline()
    for i in range(625):
        c.sendline('$')
        c.recvuntil('It will be:')
        c.sendline('1')
        temp_result = c.recvline()
        result.append(int(temp_result[:-1].replace('|', ""),16))

if __name__=="__main__":
    promo(c)
    attack(c)
    for i in range(625):
        predictor.setrandbits(result[i],32)
    print(result)
    final=predictor.getrandbits(32)
    c.sendline('$')
    c.recvuntil('It will be:')
    c.sendline(hex(final)[2:])
    print(c.recvline())
```

关于mt19937predictor可查看这个

答案

flag{6169ce2a-c2f5-46cf-9094-fa83b3b3c066}