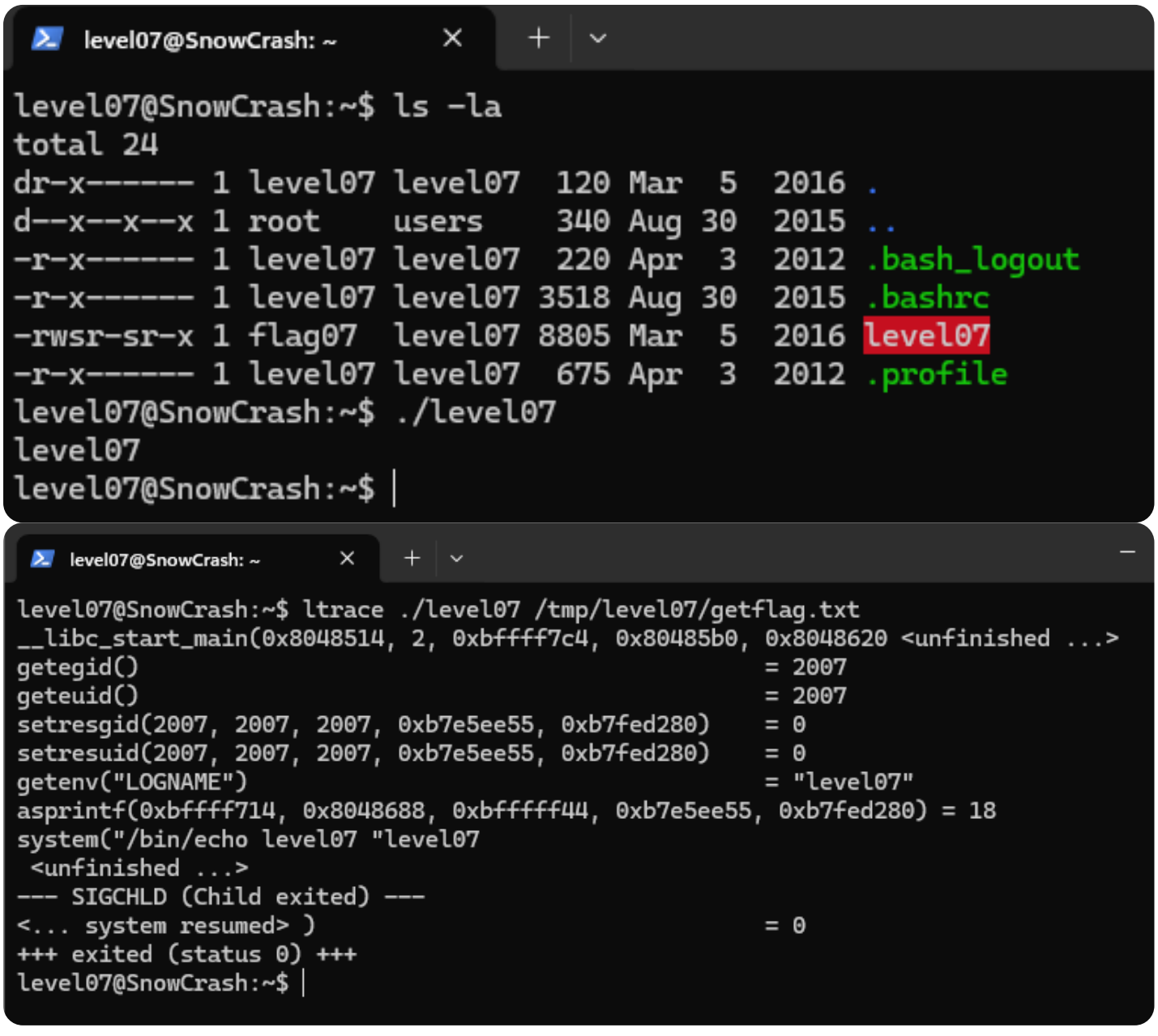
Level07

Découverte de la vulnérabilité



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.