



Level00

En el primer nivel tendremos que hacer un find desde la raíz buscando archivos del usuario flag00.

```
find -user flag00 2>/dev/null
```

```
level00@SnowCrash: /  
level00@SnowCrash:/$ find -user flag00 2>/dev/null  
./usr/sbin/john  
./rofs/usr/sbin/john  
level00@SnowCrash:/$ |
```

Con esto vemos esos dos ficheros, si hacemos un cat del primer fichero veremos que dentro tiene una string.

```
level00@SnowCrash: /  
level00@SnowCrash:/$ cat /usr/sbin/john  
cdiiddwpgswtgt  
level00@SnowCrash:/$ |
```

Viendo ese string podemos ver que está encriptado.

Uno de los encriptados mas simples que existen es el **caesar** encrypt, usando una herramienta de rot13 iremos viendo la rotación que tiene hasta que nos cuadre alguna contraseña.

En este caso, aplicando un rot11 vemos que el texto que nos da es:

nottoohardhere

rot13.com

[About ROT13](#)

The screenshot shows the rot13.com website interface. At the top, there is a text input field containing the encrypted string 'cdiiddwpgswtgt'. Below this field is a dropdown menu with 'ROT11' selected. An arrow points down from the dropdown to another text input field at the bottom, which displays the decrypted string 'nottoohardhere'.

Si insertamos `nottoohardhere` como pass de flag00 podremos acceder al usuario para ejecutar `getflag` y obtener el token de acceso al siguiente reto.