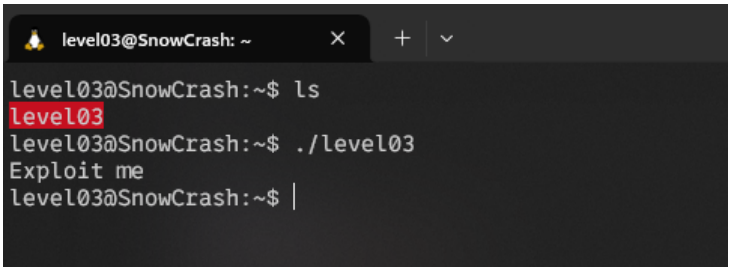
3️⃣

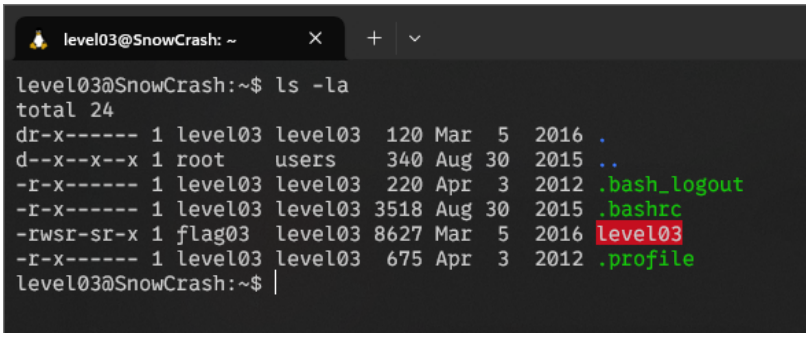
Level03

En este nivel tras entrar en la carpeta del usuario y hacer un ls vemos un binario el cual podemos ejecutar. Cuando lo ejecutamos nos muestra lo siguiente:



Esta información ya nos deja ver que el binario tendremos que usarlo para poder obtener nuestra flag o nuestro token.

Si hacemos un ls -la podremos ver que el binario tiene como dueño al usuario `flag03` esto nos hace pensar que tendremos que usarlo para ejecutar el comando `getflag`.

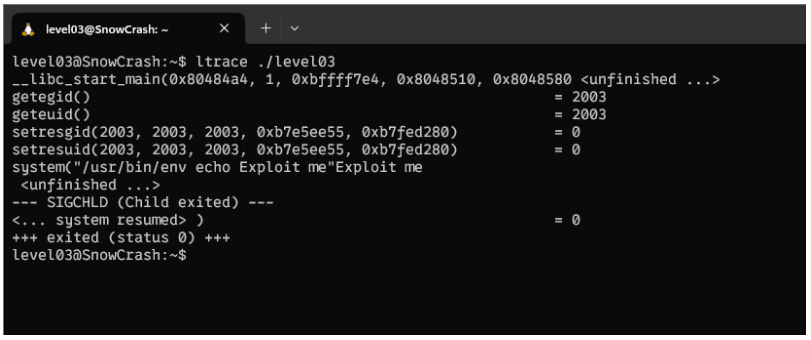


En primer lugar ejecutamos un `$ file level03` este comando nos permite ver información que pueda ser util pero a simple vista no encontramos nada.

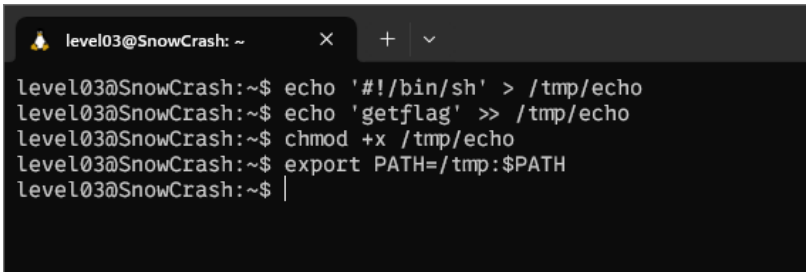
Lo siguiente que podemos hacer es usar `ltrace` para poder ver si el binario hace alguna llamada alguna función interesante, para ello ejecutamos el siguiente comando:

```
ltrace ./level03
```

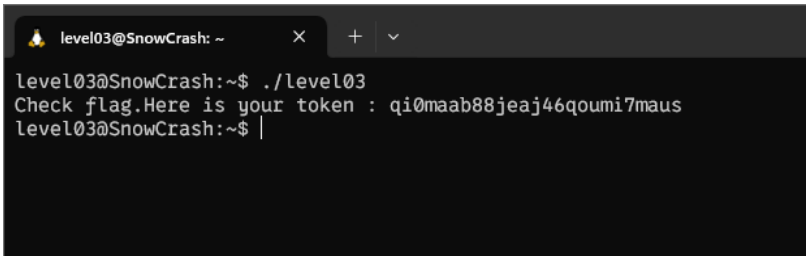
Este comando nos saca información bastante interesante, como por ejemplo que el script está haciendo una llamada a `echo` con system para poder mostrar un mensaje.



Viendo esto lo que voy a hacer va a ser crear un script básico que voy a almacenar en tmp y luego cambiar el path para añadir mi nuevo programa como si fuera echo.



Por último tan solo tendremos que ejecutar el binario para que nos de la flag.



Con esto ya sabemos que la flag es: `qi0maab88jeaj46qoumi7maus`