El clásico

Antes de ejecutar cualquier binario, se verifica qué tipo de archivo es usando file:

```
└─$ file clasico
clasico: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x
86-64.so.2, BuildID[sha1]=bae6f7b0931c17a44555c300bf307d8cad95570d, for GNU/Linux 3.2.0, not stripped
```

Esto indica que se trata de un ejecutable ELF para Linux, de 64 bits, y que no está ofuscado ni stripped, lo que facilita el análisis.

Se otorgan permisos de ejecución y se prueba el binario, el programa solicita una contraseña lo que Esto que el binario realiza una comparación directa de cadenas.

```
┌──(vfric㉿vfric)-[~/…/CTF-cyberminds-1er-Edici-n/Reverse/El clásico/Solucion]
└─$ chmod +x clasico

┌──(vfric㉿vfric)-[~/…/CTF-cyberminds-1er-Edici-n/Reverse/El clásico/Solucion]
└─$ ./clasico
Introduce la contraseña:
> l
Incorrecto.
```

Dado que es un reto de reversing básico, se utiliza la herramienta strings para extraer texto legible embebido en el binario:

```
└─$ strings clasico
/lib64/ld-linux-x86-64.so.2
mgUa
fgets
stdin
puts
strcspn
__libc_start_main
__cxa_finalize
printf
strcmp
libc.so.6
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
FIS{p4ssw0rd_h4rdc0d3d}
Introduce la contrase
Correcto! Flag: %s
Incorrecto.
```

Para filtrar directamente la flag:

strings clasico | grep FIS

Flag: FIS{p4ssw0rd_h4rdc0d3d}