

Log Hunt - PicoCTF

5na1d3r
1 de marzo de 2026

1 Introducción

Primeramente observamos que en el reto ya nos da una pista al decirnos "Our server seems to be leaking pieces of a secret flag in its logs", con eso ya sabemos que tenemos que armar la flag que esta en pedazos dentro del log, vamos a darle un vistazo al archivo.

2 Revisión del archivo

- Como primera impresión observamos que hay filas interesantes y con un formato familiar a las flags de Pico CTF.

```
1 [1990-08-09 10:00:10] INFO FLAGPART: picoCTF{us3_
2 [1990-08-09 10:00:16] WARN Disk space low
3 [1990-08-09 10:00:19] DEBUG Cache cleared
4 [1990-08-09 10:00:23] WARN Disk space low
5 [1990-08-09 10:00:25] INFO Service restarted
6 [1990-08-09 10:00:33] WARN Disk space low
[1990-08-09 10:00:33] ERROR Service failed to start
```

Archivo .log

- Así como en la anterior imagen hay pedazos de la flag que están por todo el log con la palabra "FLAGPART" en la misma linea, vamos a filtrar esas lineas usando grep.

```
> cat server.log | grep "FLAGPART"
[1990-08-09 10:00:10] INFO FLAGPART: picoCTF{us3_
[1990-08-09 10:02:55] INFO FLAGPART: y0urlinux_
[1990-08-09 10:05:54] INFO FLAGPART: sk1lls_
[1990-08-09 10:05:55] INFO FLAGPART: sk1lls_
[1990-08-09 10:10:54] INFO FLAGPART: cedfa5fb}
[1990-08-09 10:10:58] INFO FLAGPART: cedfa5fb}
[1990-08-09 10:11:06] INFO FLAGPART: cedfa5fb}
[1990-08-09 11:04:27] INFO FLAGPART: picoCTF{us3_
[1990-08-09 11:04:29] INFO FLAGPART: picoCTF{us3_
[1990-08-09 11:04:37] INFO FLAGPART: picoCTF{us3_
[1990-08-09 11:09:16] INFO FLAGPART: y0urlinux_
[1990-08-09 11:09:19] INFO FLAGPART: y0urlinux_
[1990-08-09 11:12:40] INFO FLAGPART: sk1lls_
[1990-08-09 11:12:45] INFO FLAGPART: sk1lls_
```

- En la anterior imagen por intuición ya podemos deducir la flag, pero para poner en práctica nuestras habilidades vamos a usar herramientas para que con una sola linea de comando nos devuelva la flag.

```
> cat server.log | grep "FLAGPART" | awk -F ':' '{print $2}' | awk '!x[$0]+  
+' | tr -d '\n' | tee /dev/tty | xclip -selection clipboard; echo  
picoCTF{us3_y0urlinux_sk1lls_cedfa5fb}
```

Obtención de la flag

- Introducimos la flag en el reto de Pico CTF para ver si realmente acabamos el reto.



picoCTF{us3_y0urlinux_sk1lls_cedfa5fb}

Submit
Flag

Introduciendo flag

- Y listo, nos salió las felicitaciones, reto resuelto.

Hurray! You
have solved
this challenge ×
correctly
again.

Reto resuelto