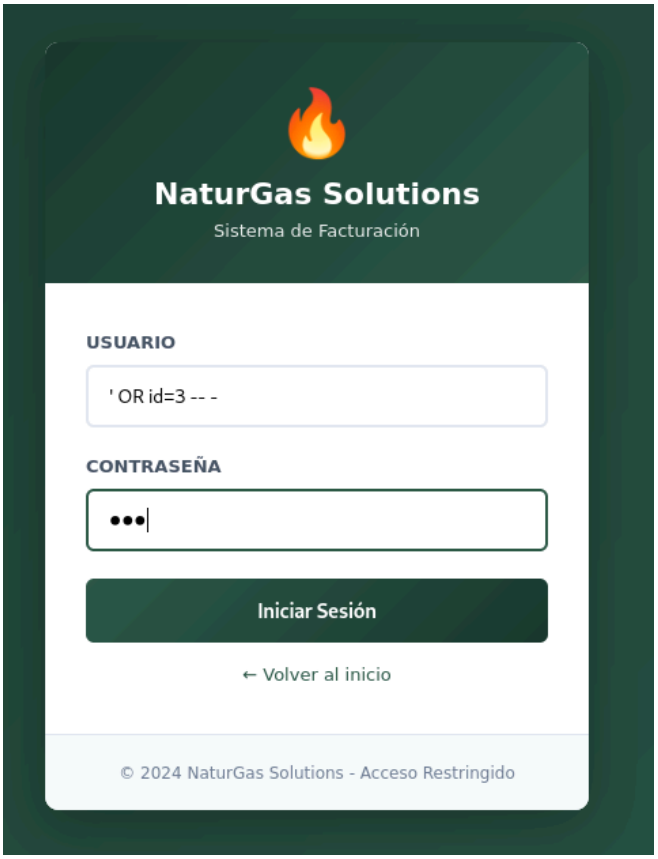
Arrancamos la máquina:

Escaneamos con nmap la máquina, para saber que servicios tiene disponibles:

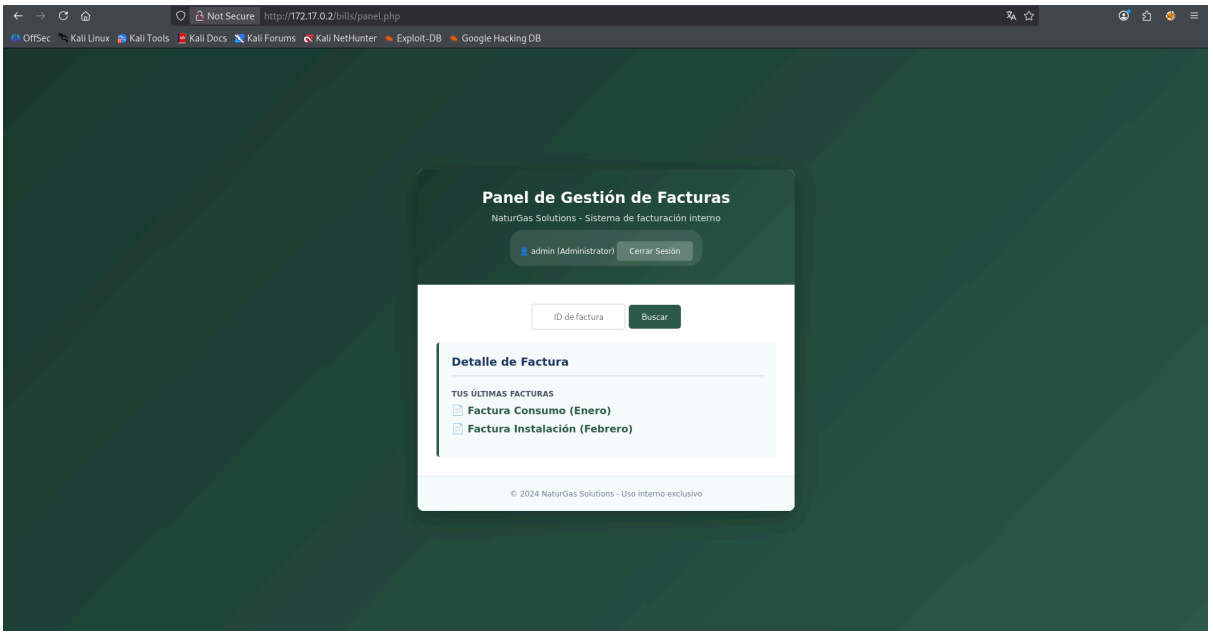
```
(kali㉿kali)-[~/dockerlabs/Fácil]
$ nmap -p- -T4 172.17.0.2
Starting Nmap 7.98 ( https://nmap.org ) at 2026-05-04 18:02 -0400
Nmap scan report for 172.17.0.2
Host is up (0.0000050s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds
```

Esta es la página principal de la máquina

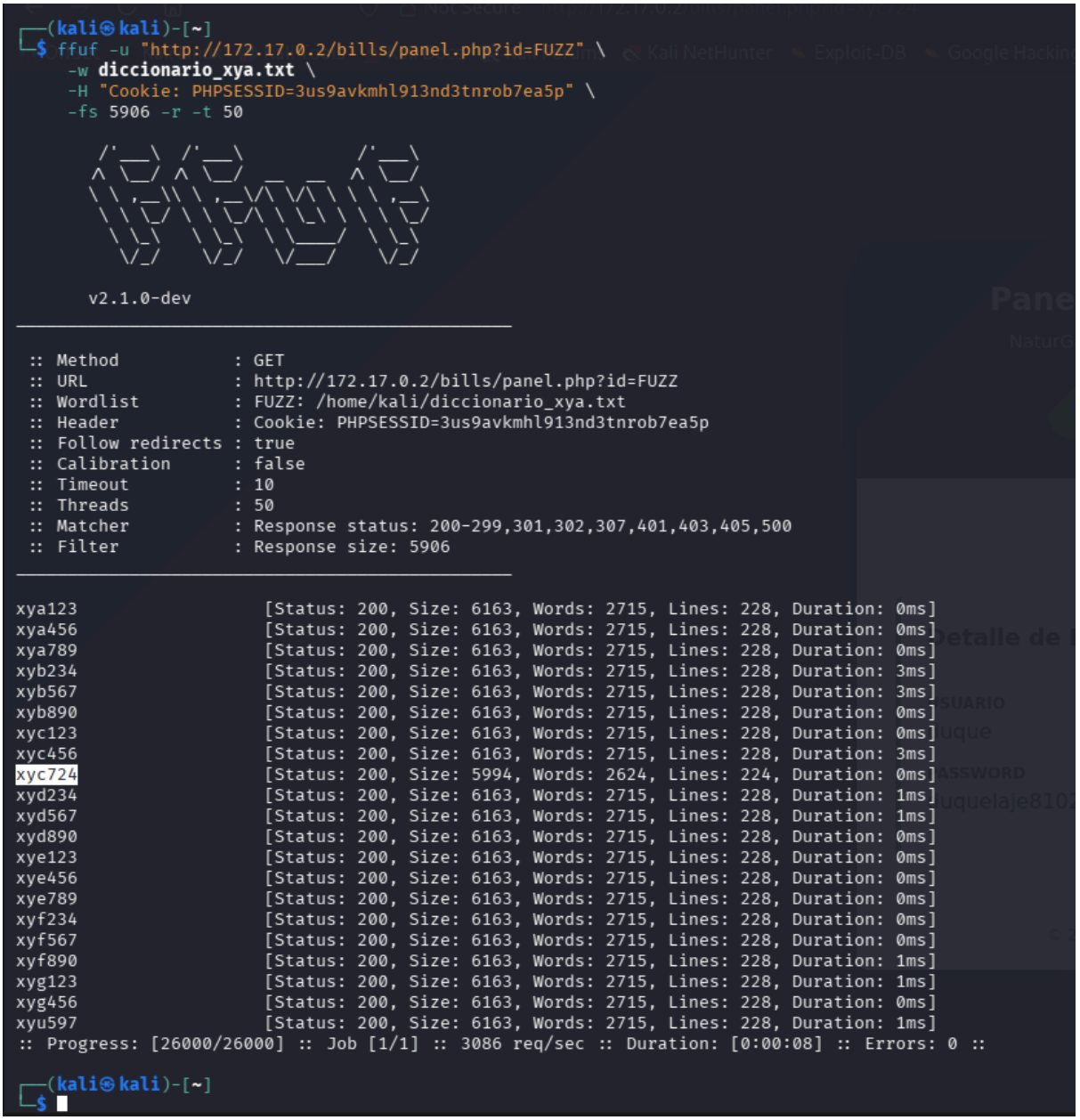
Haciendo fuerza bruta de directorios encontramos el directorio /bills/ , el cuál es vulnerable a SQL injection



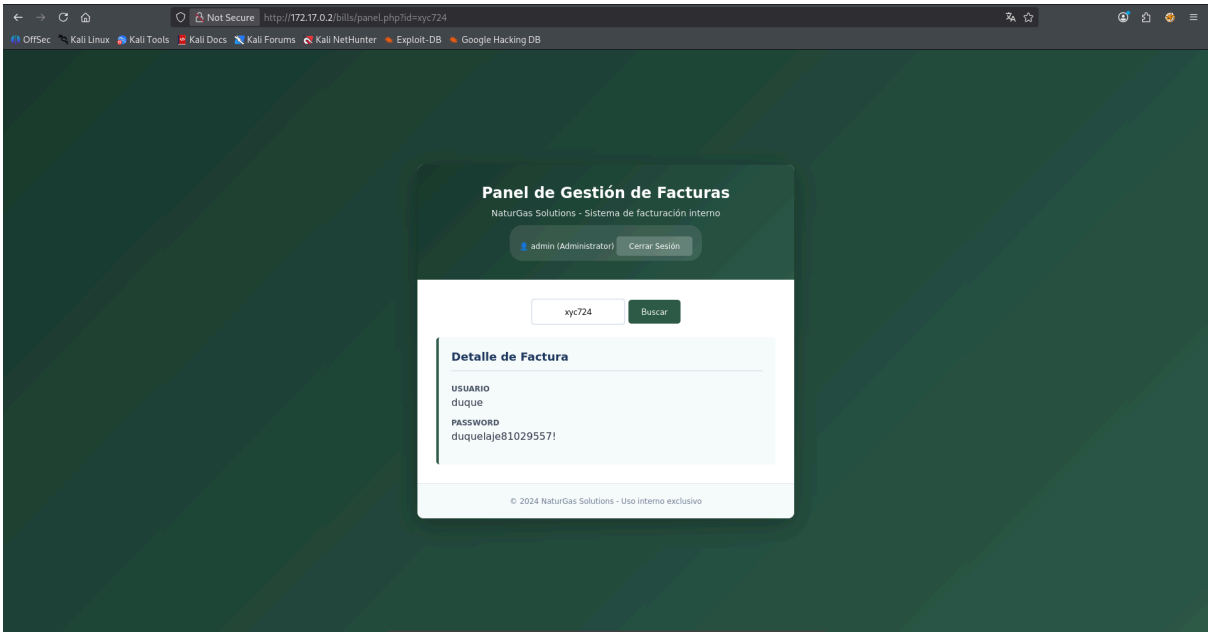
Encontramos que podemos ver facturas según su ID



Nos damos cuenta de que hay más facturas disponibles a parte de las dos que se ven, por lo que hacemos fuzz y comparamos el Size



Encontramos que una de ellas nos da un usuario y contraseña:



Nos registramos con esas credenciales por ssh:

```
┌──(kali㉿kali)-[~/dockerlabs/Fácil]
└─$ ssh duque@172.17.0.2
duque@172.17.0.2's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.18.5+kali-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Mon May  4 21:54:36 2026 from 172.17.0.1
duque@2cf3d46e2fcf:~$
```

vemos como podemos escalar privilegios:

```
duque@2cf3d46e2fcf:~$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/su
/usr/bin/env
/usr/bin/mount
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/sudo
duque@2cf3d46e2fcf:~$
```

Máquina completada, usuario root conseguido