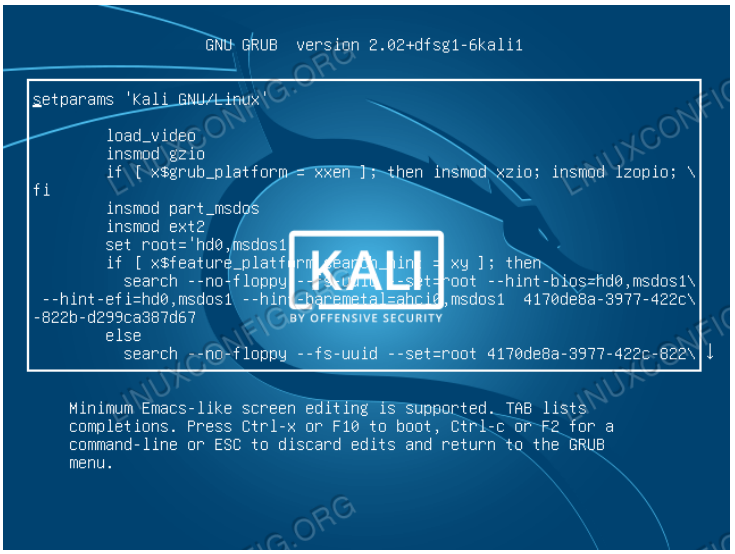
VULNHUB N7 Documentation

At First i cracked the kali linux root password using the following commands and steps

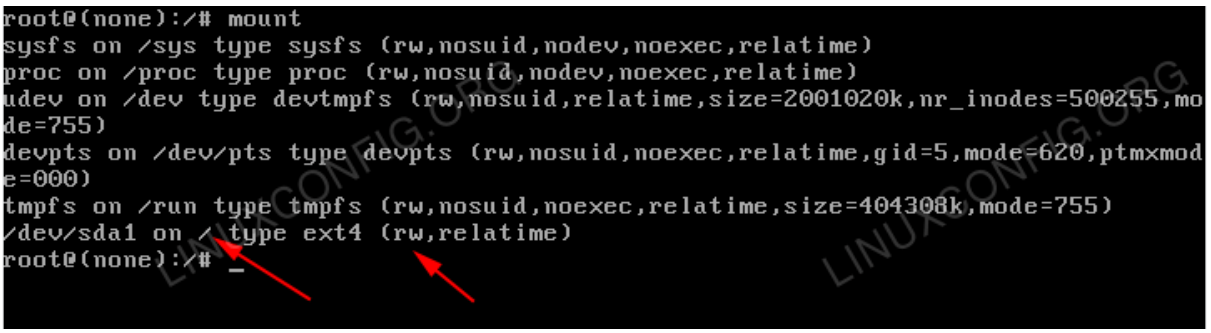
1. Reboot kali linux and press “e” while booting to edit grub boot menu entry

2. Once entering the GRUB edit mode, scroll down until you observe the line starting with linux



3. Within the line in linux you can look for keywords “ro” and replace it with keywords “rw”. Also replace “quiet” within the same line into “init=/bin/bash”. Then press enter

4. As the command prompt is shown, type mount and press enter to conform the root partition. Conform the partition is mounter with rw permission.



5. Now you are ready to reset the root user password. Here you should type “passwd” command and enter your new password. Then we would press enter and conform password reset. At last we should type reboot to boot our system.

```
root@(none):/# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=2001020k,nr_inodes=500255,mo
de=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmod
e=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=404308k,mode=755)
/dev/sda1 on / type ext4 (rw,relatime)
root@(none):/# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@(none):/#
```

Thus we have successfully changed our root password.

Now walking through the Web Machine VulNub N7

1. We should focus on the description provided by the organization.

   Here we came to know that dhcp service is enabled and ip addresses are automatically assigned. Through screenshots provided we came to know that our system is also hosting a web page

2. Checking the ip configuration of our systems

   Ifconfig can help us know about the ip address of our system. Here i can to know ip address of my system is 10.0.2.15

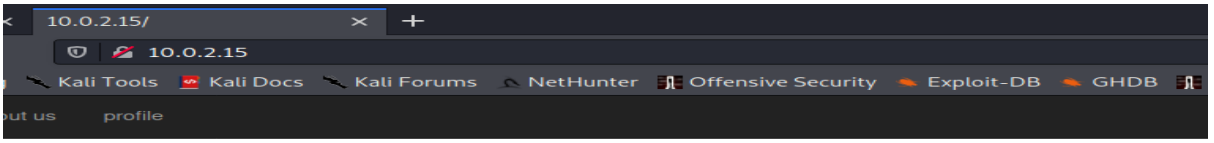
```
┌──(root㉿ kali)-[~]
└─# ifconfig
th0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:feed:bdc7  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ed:bd:c7  txqueuelen 1000  (Ethernet)
        RX packets 4  bytes 930 (930.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15  bytes 1397 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

o: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 756 (756.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 756 (756.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. Scanning using nikto (free software command line vulnurebality scanner that scan web servers for dangerous and outdated files)

```
┌──(root㉿ kali)-[~]
└─# nikto -h 10.0.2.15
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.0.2.15
+ Target Hostname:    10.0.2.15
+ Target Port:        80
+ Start Time:         2023-08-14 03:39:38 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.46 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agen
t to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to
render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 654, size: 5cf
8ad59e198a, mtime: gzip
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
```

4. Here as we know our server is being hosted, i used my device ip to check if it is hosted and hurray, it is opened.

```
└─# firefox 10.0.2.15                                                    127 ×
Sandbox: unsupported fd-relative fstatat(27, "", 0x7FFD722CF040, 4096)
Sandbox: seccomp sandbox violation: pid 2245, tid 2245, syscall 262, args 27 139
920551854846 140726519001152 4096 4096 1.
Sandbox: unsupported fd-relative fstatat(27, "", 0x7FFE6916B190, 4096)
Sandbox: seccomp sandbox violation: pid 2288, tid 2288, syscall 262, args 27 140
021162881790 140730661515664 4096 4096 1.
[GFX1-]: Unrecognized feature VIDEO_OVERLAY
Sandbox: unsupported fd-relative fstatat(25, "", 0x7FFE105DB9B0, 4096)
Sandbox: seccomp sandbox violation: pid 2312, tid 2312, syscall 262, args 25 140
674260693758 140729172998576 4096 4096 1.
Sandbox: unsupported fd-relative fstatat(27, "", 0x7FFE13773140, 4096)
Sandbox: seccomp sandbox violation: pid 2340, tid 2340, syscall 262, args 27 140
526584902398 140729224999232 4096 4096 1.
```



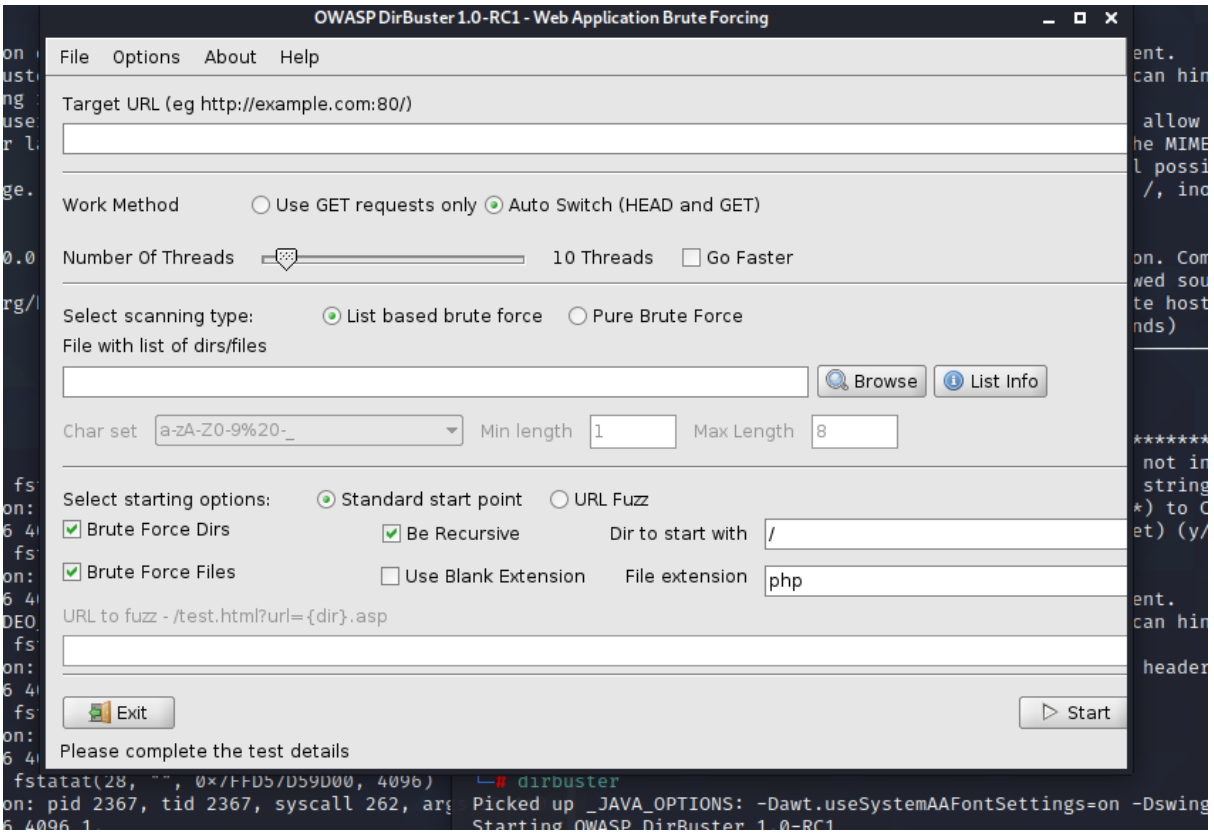
WELCOME IN BLOG

this is first blog

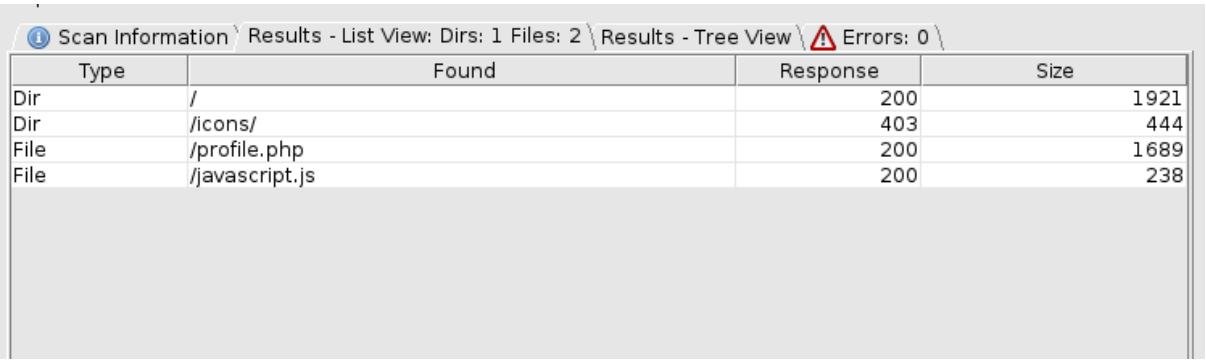
5. Here we should find to different flags to accomplish our work. As we opened our page we didnt find anything interesting to look. Thus we are using dirbuster to locate the directory and files

```
┌──(root㉿ kali)-[~]
└─# dirbuster
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Starting OWASP DirBuster 1.0-RC1
```

It would open using dirbuster in gui.



6. Now here we would be placing our ip and wordlists downloaded from the browser. The output of dirbuster are observed belo as

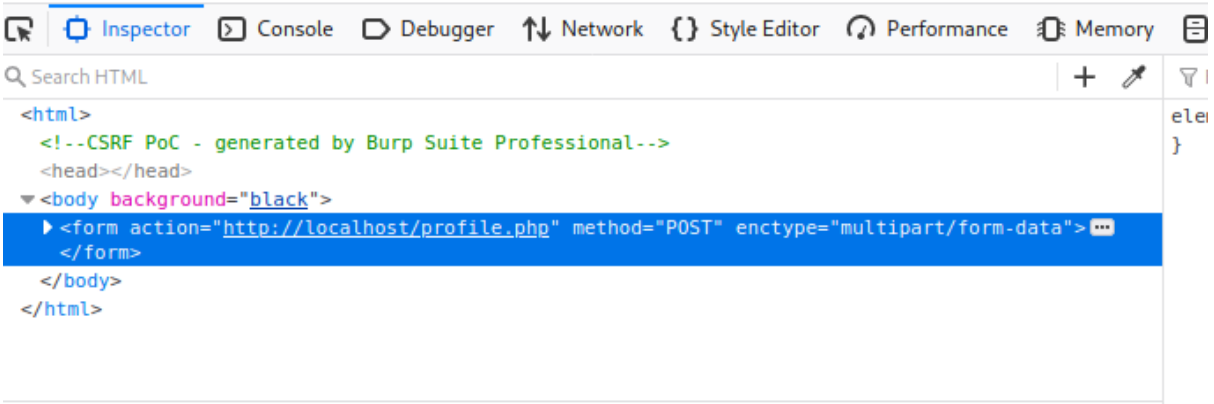


Scan Information | Results - List View: Dirs: 1 Files: 2 | Results - Tree View | Errors: 0

Type	Found	Response	Size
Dir	/	200	1921
Dir	/icons/	403	444
File	/profile.php	200	1689
File	/javascript.js	200	238

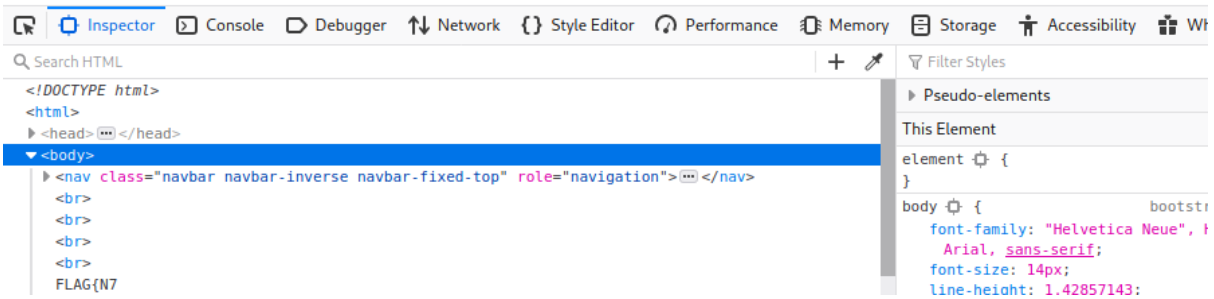
7. While scanning using dirbuster, we observer http://10.0.2.15/exploit.html as one of the links there. While inspecting the source of the page, we observe the page is being hosted using local host but we have our own ip. Thus changing the local host

into our own ip.

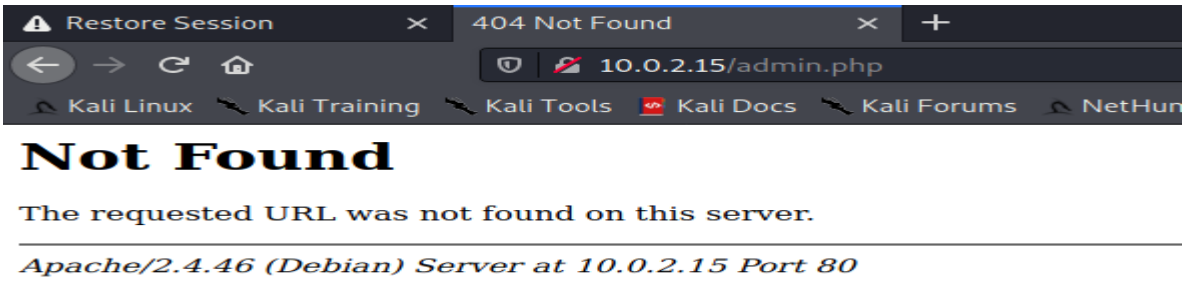


As soon as we changed localhost into our own ip and pressed enter we have got our first flag

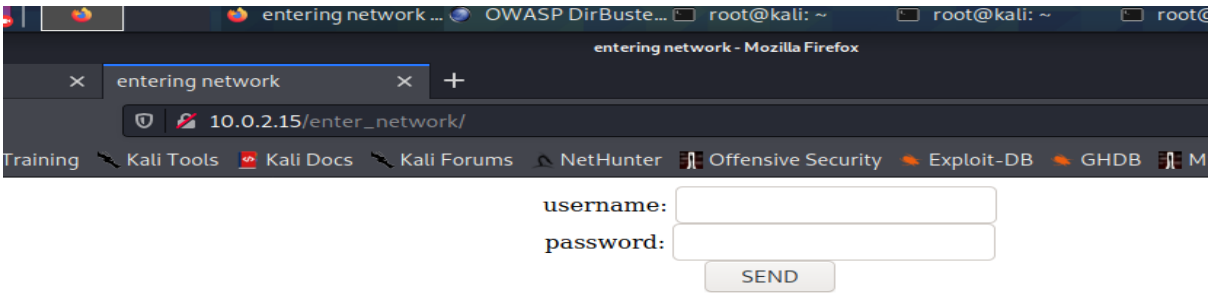
FLAG{N7



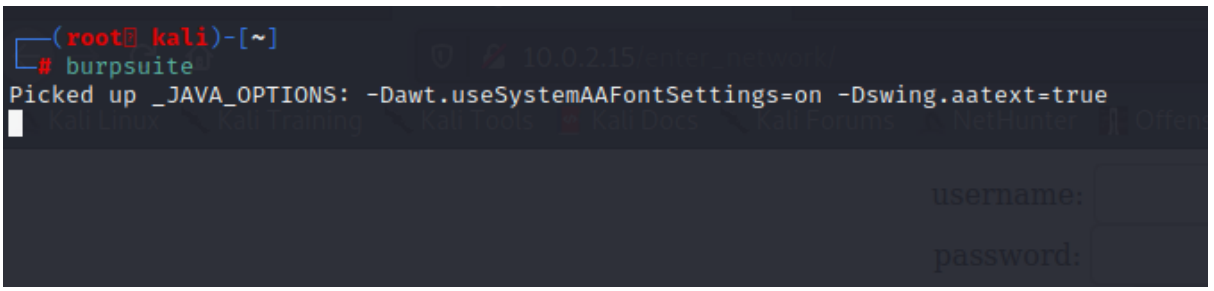
8. Now moving forward We have also observer /admin.php, while click it shows forbiddenpage



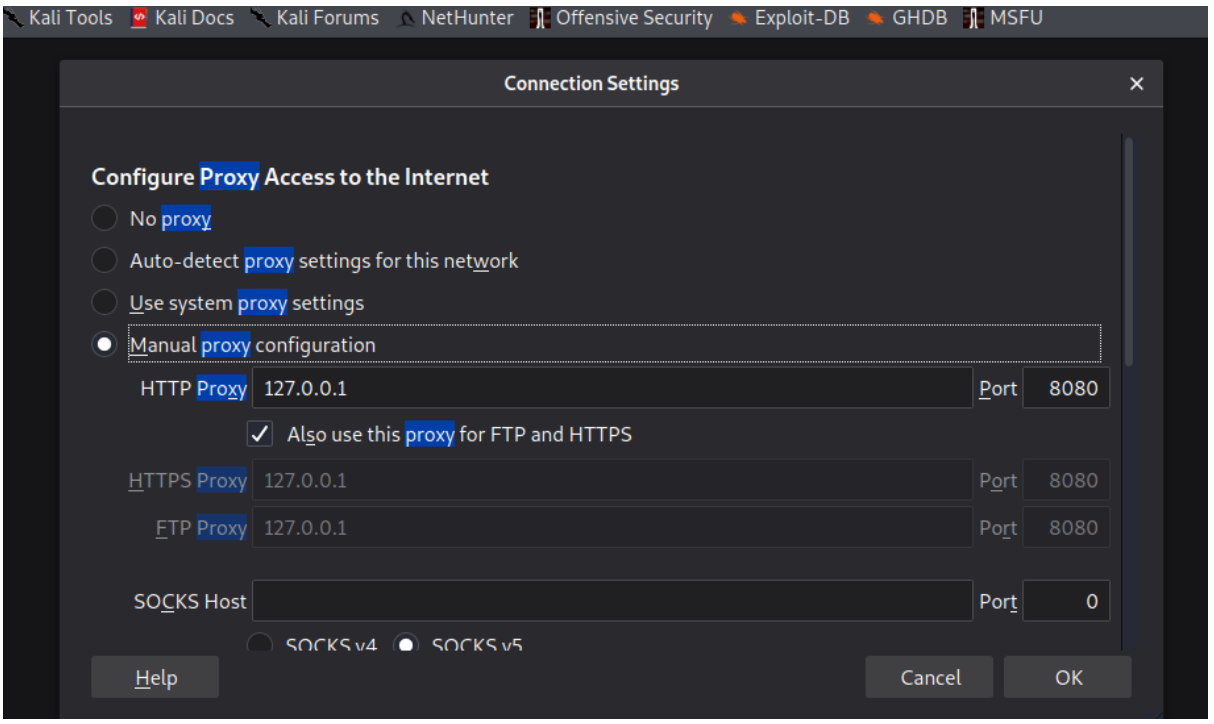
Also we can observe there are other link such as http://10.0.2.15/enter_network/



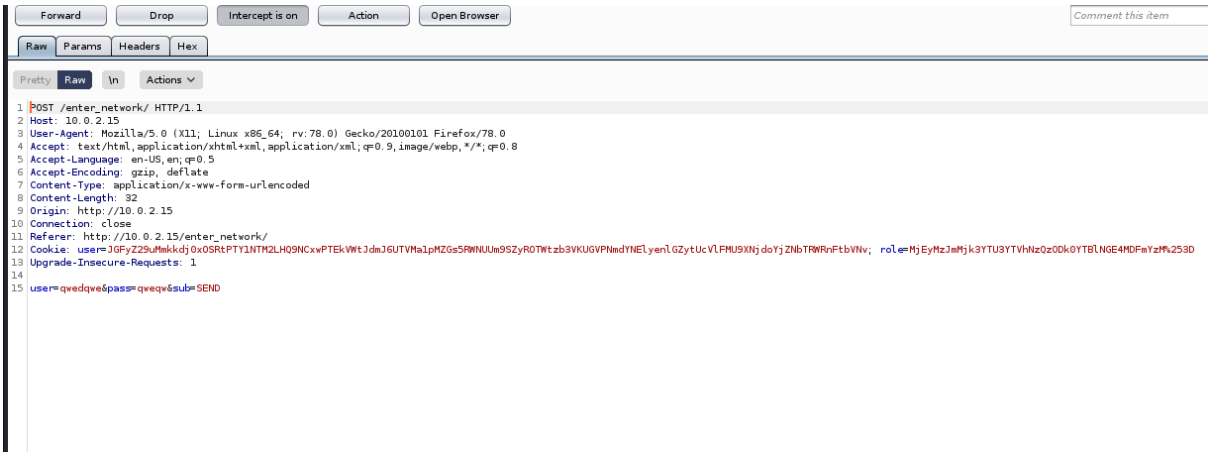
Now using brupsuite to set proxy and acces the page.



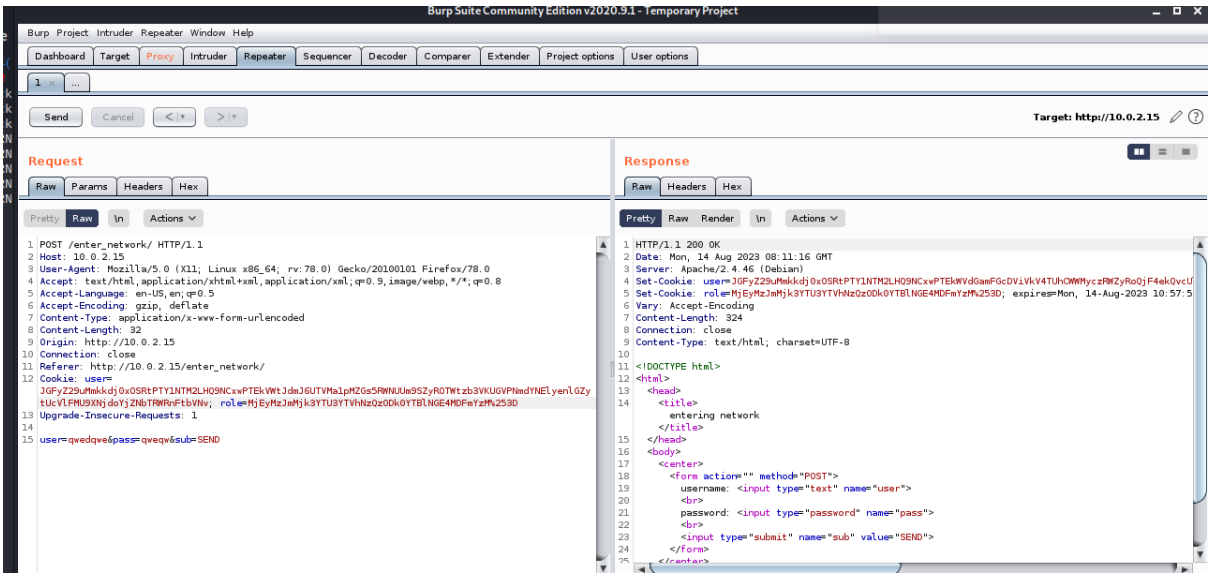
9. Proxy are set by going to setting in the browser and changing proxy in the preference section



10. While manual proxy are set, you can observe burpsuite. Making the intercept on

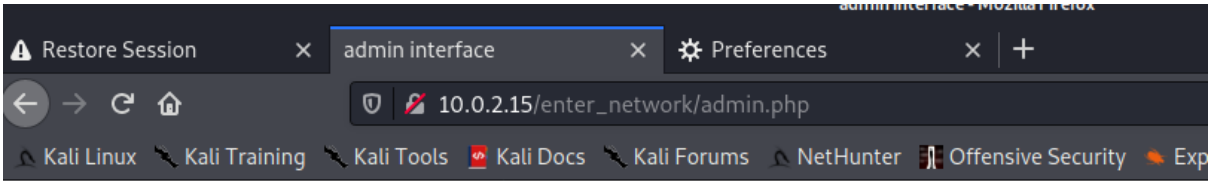


Sending it to intruder



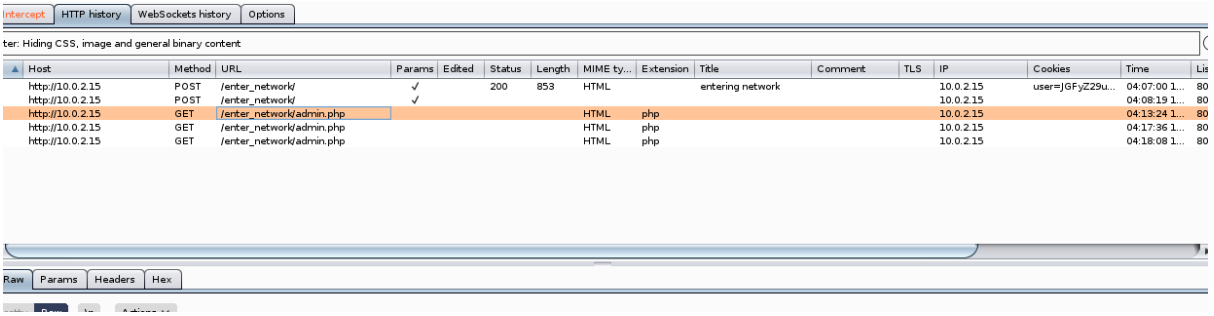
No any changes were observer.

11. Thus now opening http://10.0.2.15/enter_network/admin.php

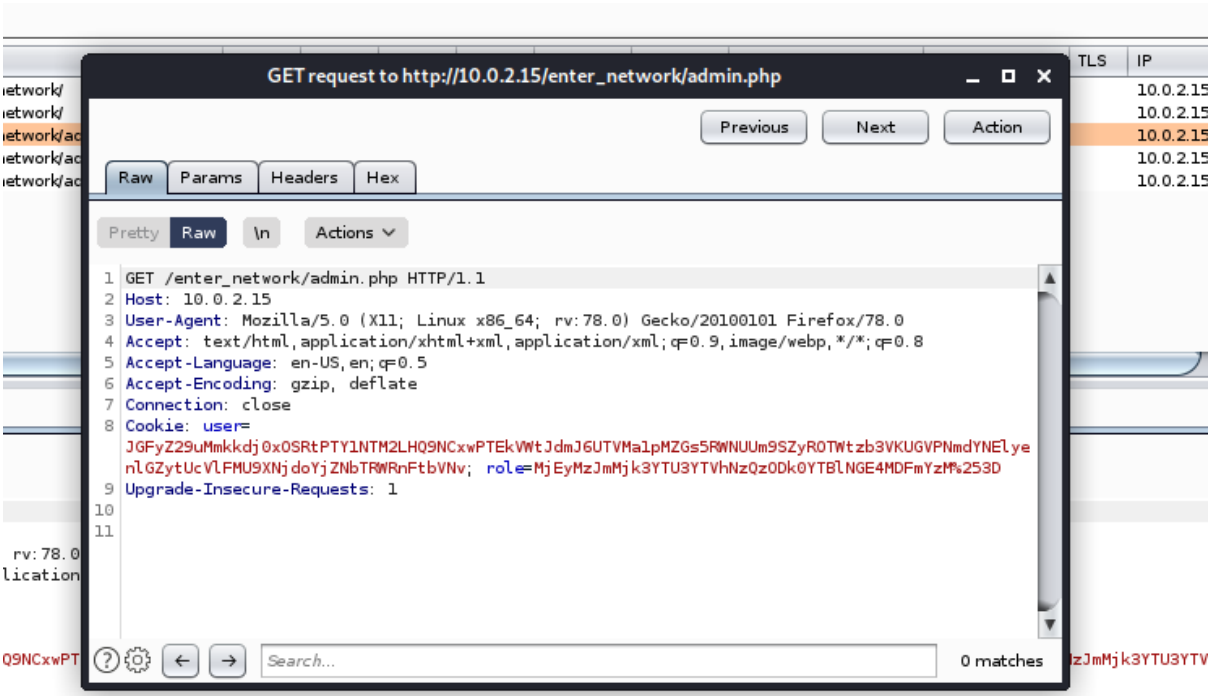


this interface is admin only

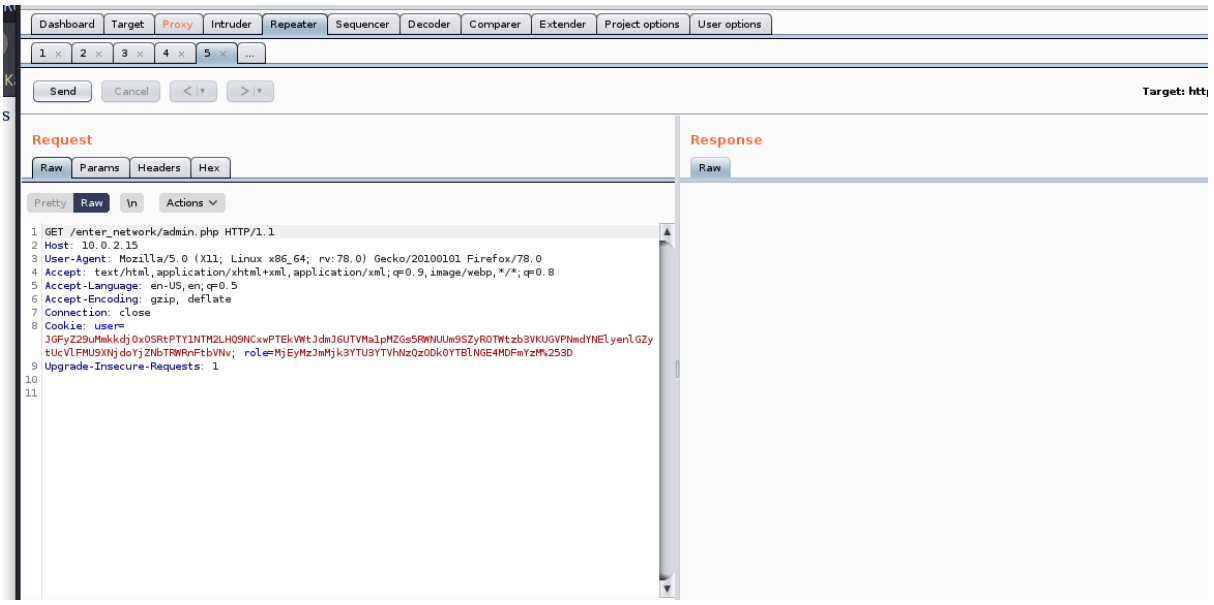
12. Opening the burpsuit and checking the proxy in it the, we can observe the web page we are looking for.



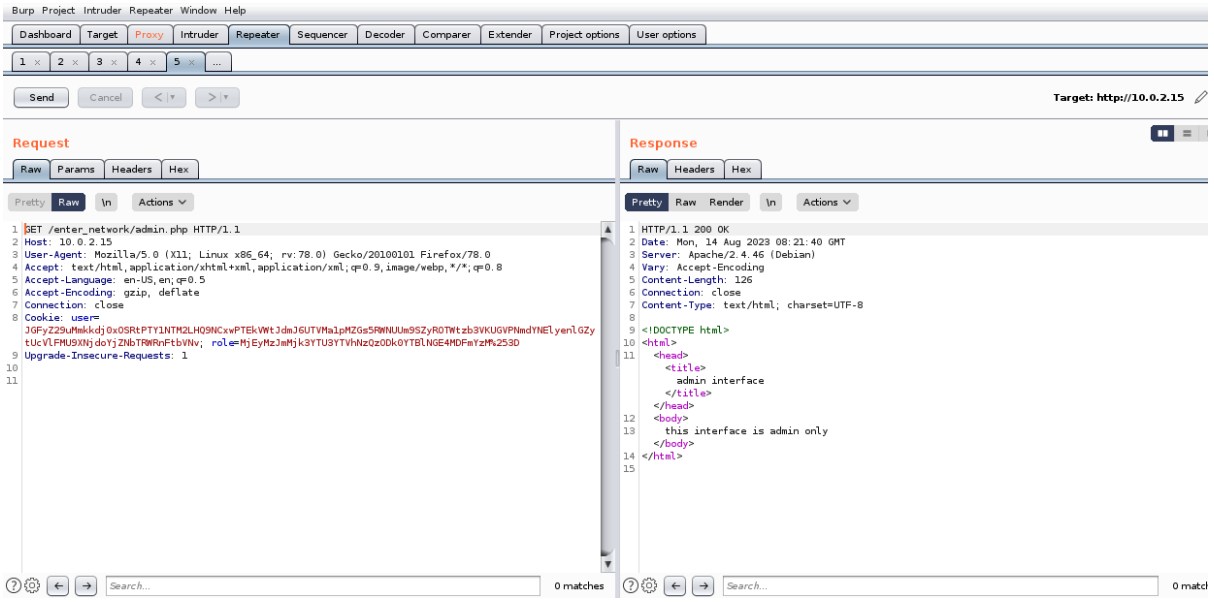
13. Now clicking on the web address we can get the following



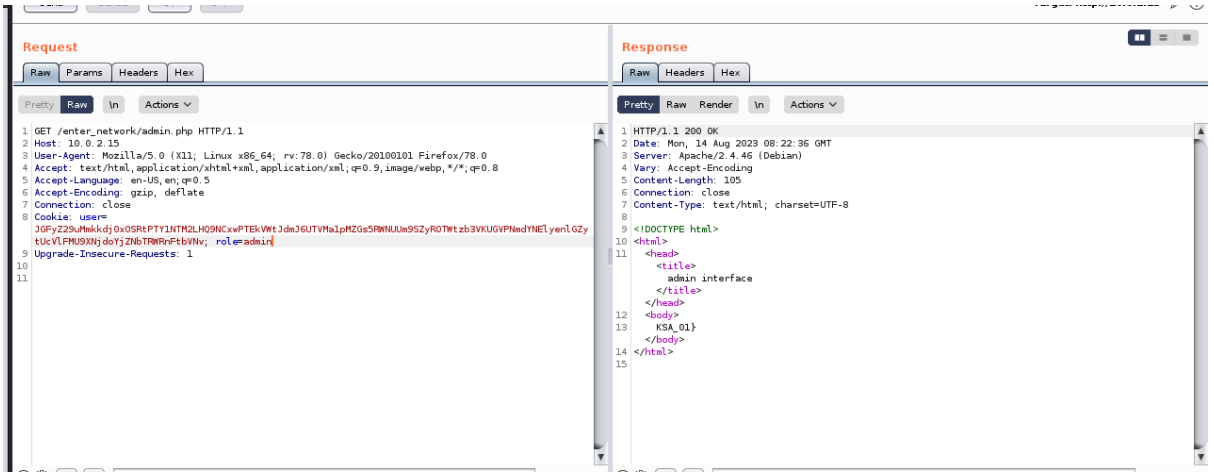
14. Sending it to the repeater, we will observer the following



15. Pressing send button we will observe the following



16. Since only the root permission are provided, we will change the role into admin and observer the output



17. Here we can see the body has been changed and tahts the flags.

Thus our two flags within the web machine are

FLAG{N7