

# TryHackMe: Simple CTF Writeup

Author: Amal Pradeep

Room: Simple CTF

Date: July 13, 2025

## 1. Overview

This document presents a walkthrough of the TryHackMe 'Simple CTF' room, which involved discovering open services, exploring web vulnerabilities, and analyzing CMS versions. Although the exploitation step was skipped intentionally, the key enumeration and discovery phases were completed.

## 2. Tools Used

- Nmap
- Gobuster
- Firefox (in TryHackMe AttackBox)
- Linux Terminal

## 3. Screenshots & Steps

*Nmap scan showing open ports and service versions*

```
Applications Places Sat 12 Jul, 12:17 AttackBox IP:10.10.169.67
root@ip-10-10-169-67: ~
File Edit View Search Terminal Help
21/tcp open ftp vsftpd 3.0.3
ftp-anon: Anonymous FTP login allowed (FTP code 230)
_Can't get directory listing: TIMEOUT
ftp-syst:
STAT:
FTP server status:
  Connected to ::ffff:10.10.169.67
  Logged in as ftp
  TYPE: ASCII
  No session bandwidth limit
  Session timeout in seconds is 300
  Control connection is plain text
  Data connections will be plain text
  At session startup, client count was 3
  vsFTPD 3.0.3 - secure, fast, stable
_End of status
20/tcp open http Apache httpd 2.4.18 ((Ubuntu))
http-robots.txt: 2 disallowed entries
_/ /openemr-5_0_1_3
_http-server-header: Apache/2.4.18 (Ubuntu)
_http-title: Apache2 Ubuntu Default Page: It works
222/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
  256 9b:d1:65:07:51:08:00:61:98:de:95:ed:3a:e3:81:1c (ECDSA)
  256 12:65:1b:61:cf:4d:e5:75:fe:f4:e8:d4:6e:10:2a:f6 (ED25519)
MAC Address: 02:15:36:B7:A7:91 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.22 seconds
root@ip-10-10-169-67:~#
```

*Apache default page shown in browser*


Applications Places Sat 12 Jul, 12:21 AttackBox IP:10.10.169.67

Apache2 Ubuntu Default Page: It works — Mozilla Firefox

Apache2 Ubuntu Default Pa X +

← → ↻ 🏠 10.10.162.136 ☆ 📧 📁 📌 ≡

TryHackMe | Learn Cy... TryHackMe Support 📄 Offline CyberChef 🌐 Revshell Generator >>



# Apache2 Ubuntu Default Page

## ubuntu

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

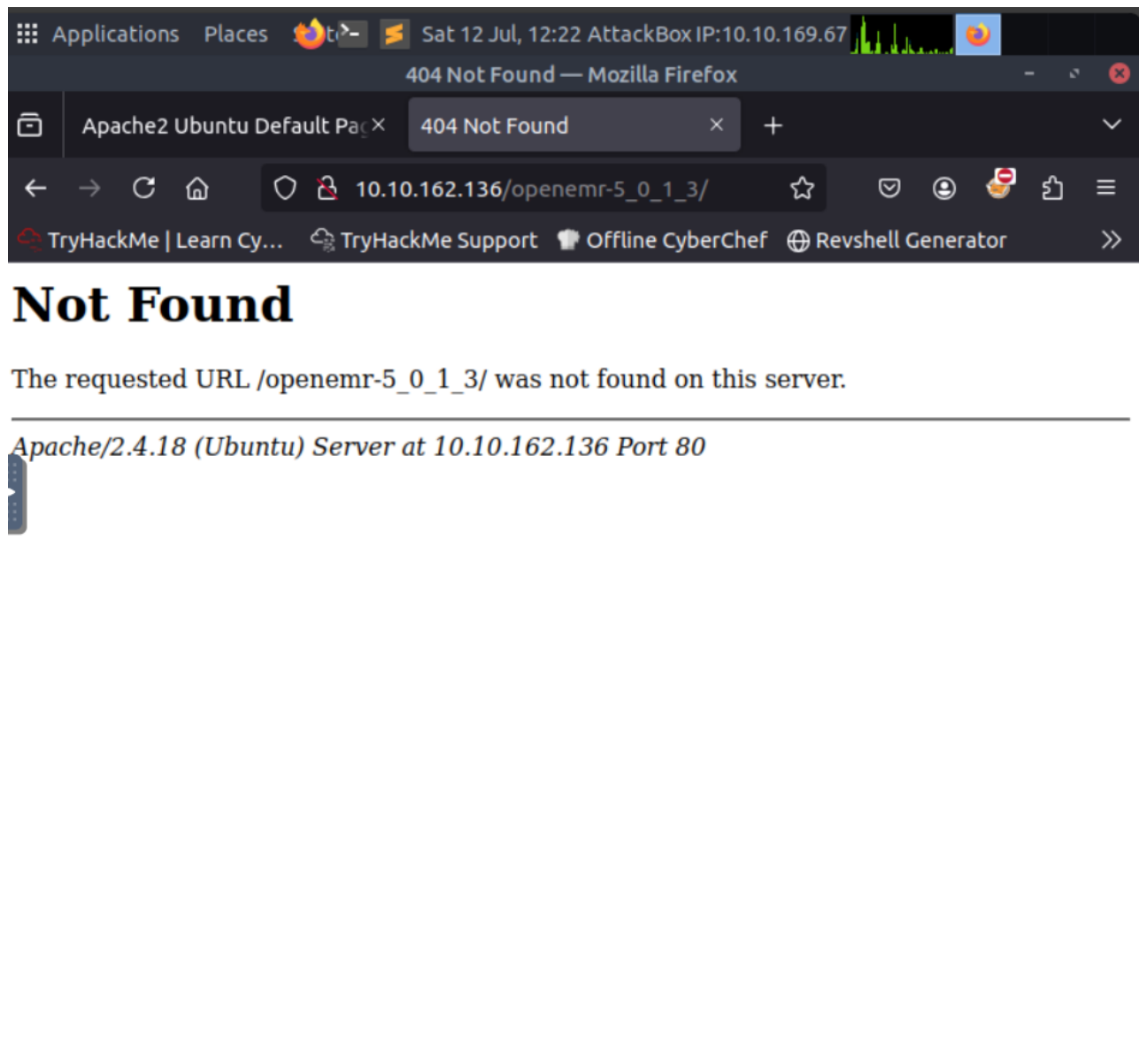
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|   |-- ports.conf  
|-- mods-enabled
```

*Gobuster directory enumeration results*

```
Applications Places Sat 12 Jul, 12:28 AttackBox IP:10.10.169.67
root@ip-10-10-169-67: ~
File Edit View Search Terminal Help
^C
--- 10.10.162.136 ping statistics ---
530 packets transmitted, 530 received, 0% packet loss, time 538230ms
rtt min/avg/max/mdev = 0.276/0.684/4.732/0.343 ms
root@ip-10-10-169-67:~# gobuster dir -u http://10.10.162.136 -w /usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.162.136
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta (Status: 403) [Size: 292]
/.htpasswd (Status: 403) [Size: 297]
/.htaccess (Status: 403) [Size: 297]
/index.html (Status: 200) [Size: 11321]
/robots.txt (Status: 200) [Size: 929]
/server-status (Status: 403) [Size: 301]
/simple (Status: 301) [Size: 315]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====
root@ip-10-10-169-67:~#
root@ip-10-10-169-67:~# ^C
root@ip-10-10-169-67:~#
```

*Attempt to access /openemr-5\_0\_1\_3/ returns 404 Not Found*



## 4. Conclusion

The Simple CTF room was a valuable introduction to CTF-style challenges. The user successfully discovered accessible services, web directories, and identified a vulnerable CMS version (CMS Made Simple 2.2.8), which is known to be vulnerable to SQL injection.