Creating a CTF

PART 1: The end result

Category of the CTF

Steganography

Creator of the CTF

Robin Swolfs

Title of the CTF

Home is where the heart is

Story to guide the CTF

Welcome in my tiny cozy home where nothing is as it seems. But it's sooo hot inside! Maybe open up a window?

Difficulty level of the CTF

🌶🌶🌶 *(if not skilled)*
🌶🌶 *(if skilled)*

Needed Starting files to complete the CTF

ctf.xcf

The flag which can be found in the CTF

flag{home_SWEET_home}

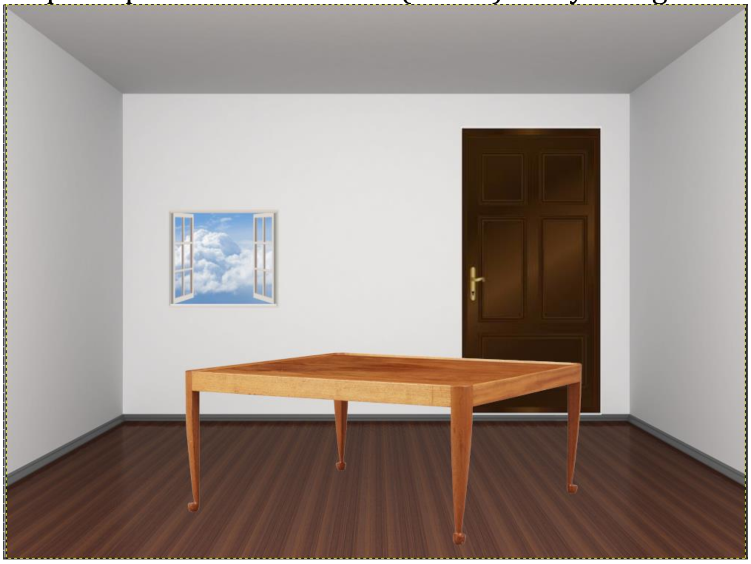
PART 2: Solution of the CTF

Which tools are needed

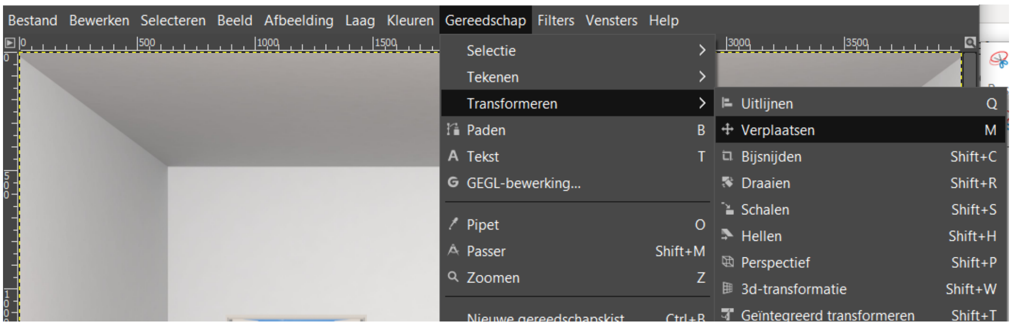
Open source photoshop program called "Gimp"
Dirbuster

The solution

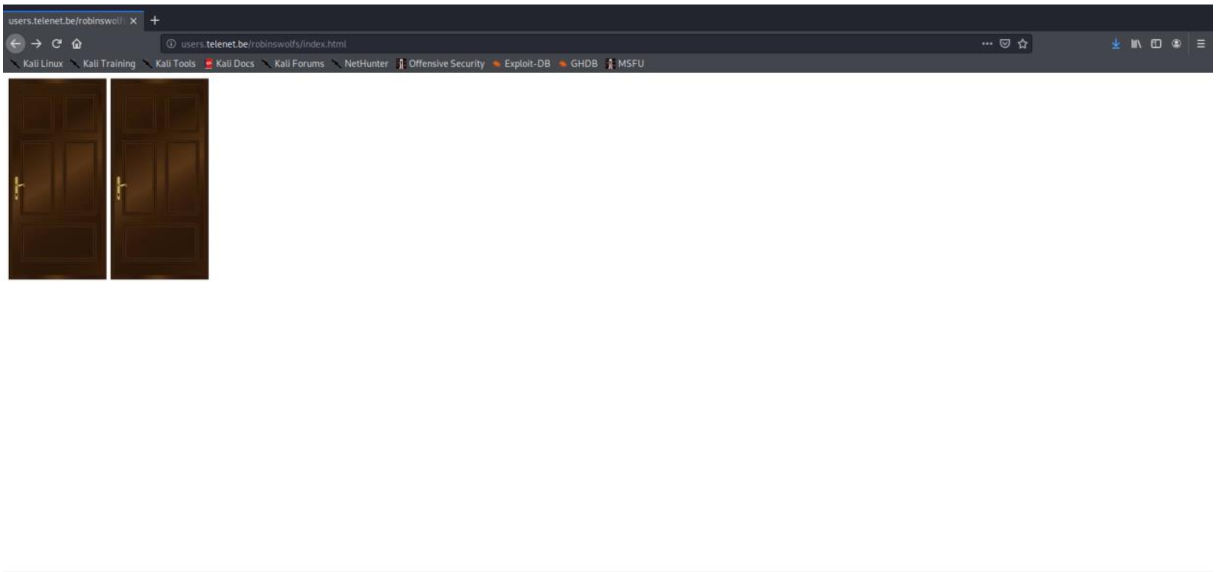
Step 1: Download GIMP
Step 2: Open the file in GIMP (ctf.xcf) and you'll get a room



Step 3: Remove the window by dragging it away or deleting the layer. You can click on "gereedschap" and then "transform" and finally "verplaatsen"

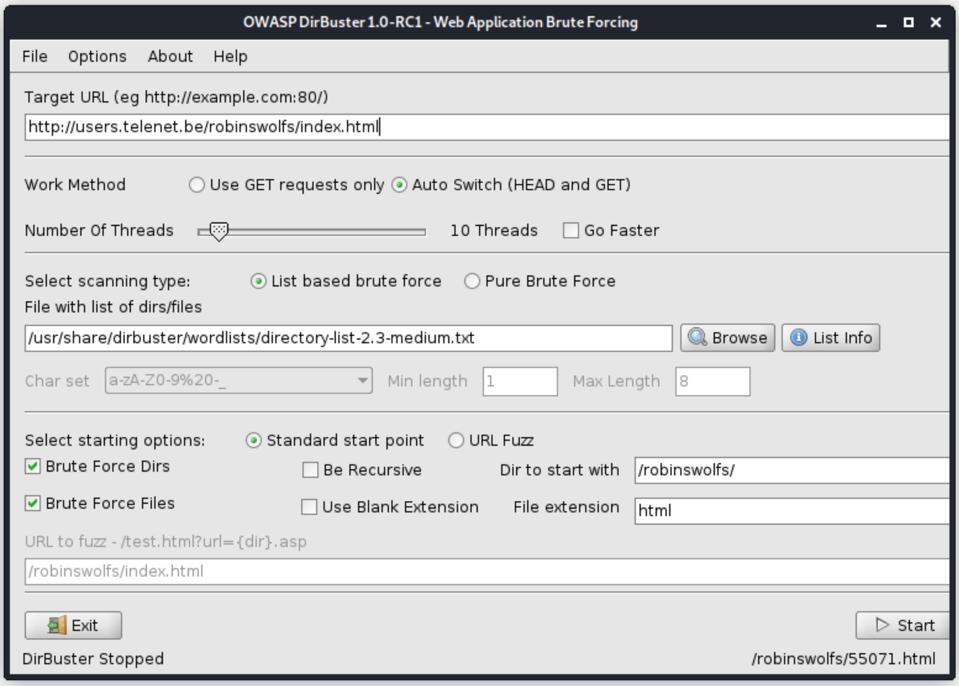


Step 4: Scan the qr code and get trolled! You can just use the camera of your phone.
Step 5: Same as step 3 but now on the door
Step 6: Scan the qr code and go to the site. The site is http://users.telenet.be/robinswolfs/index.html



Step 7: You can use the different doors, but there's nothing important there. After the right door is an important hint. Bust some dirs!

Step 8: Use dirbuster to find a hidden file called "secret.html". But first you'll need to use the correct settings.



Target URL (eg http://example.com:80/)
http://users.telenet.be/robinswolfs/index.html

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs □ Be Recursive Dir to start with /robinswolfs/

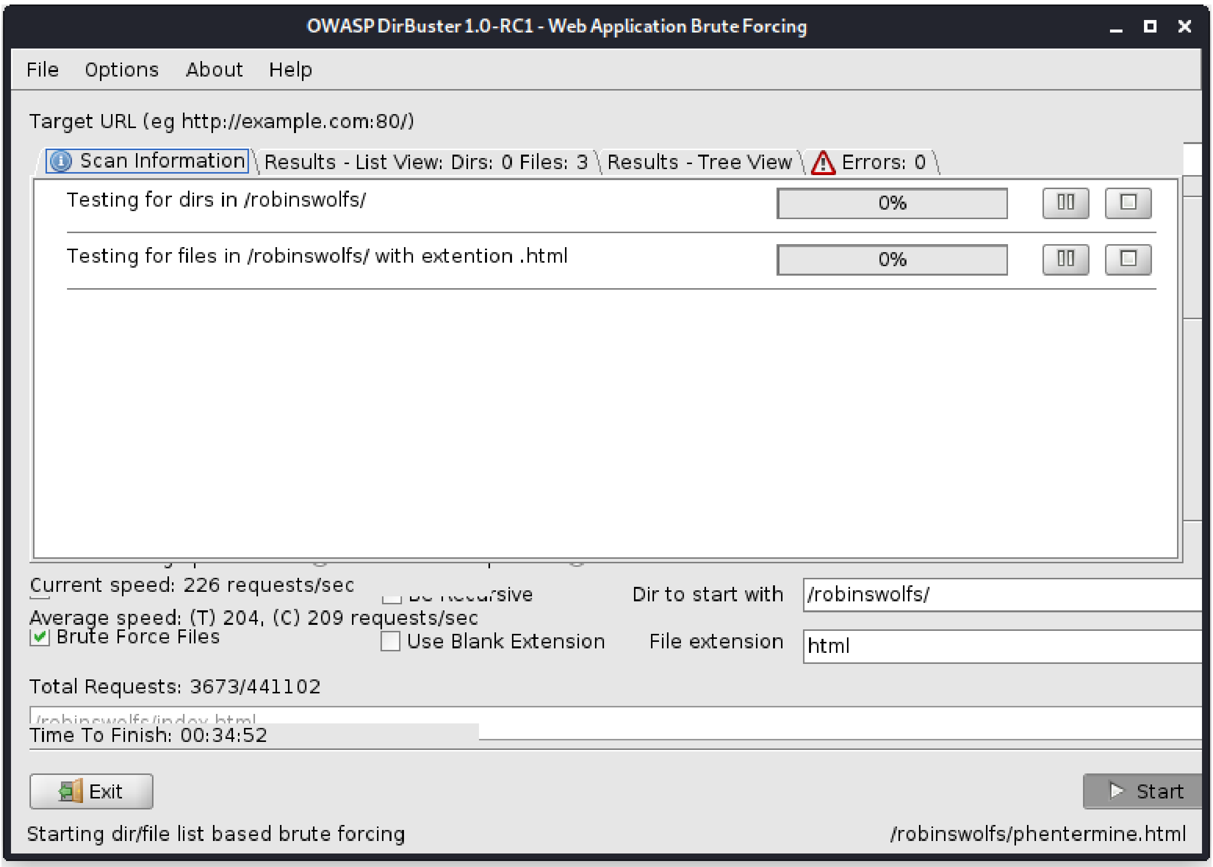
☑ Brute Force Files □ Use Blank Extension File extension html

URL to fuzz - /test.html?url={dir}.asp
/robinswolfs/index.html

DirBuster Stopped /robinswolfs/55071.html

We don't want to use recursive searching and the file extension is of course html instead of php.

Now start the busting!


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Scan Information
Results - List View: Dirs: 0 Files: 3
Results - Tree View
Errors: 0
Exit
Start

Target URL (eg http://example.com:80/)

Testing for dirs in /robinswolfs/ 0%

Testing for files in /robinswolfs/ with extention .html 0%

Current speed: 226 requests/sec

Average speed: (T) 204, (C) 209 requests/sec

☑ Brute Force Files

□ Use Blank Extension

Dir to start with /robinswolfs/

File extension html

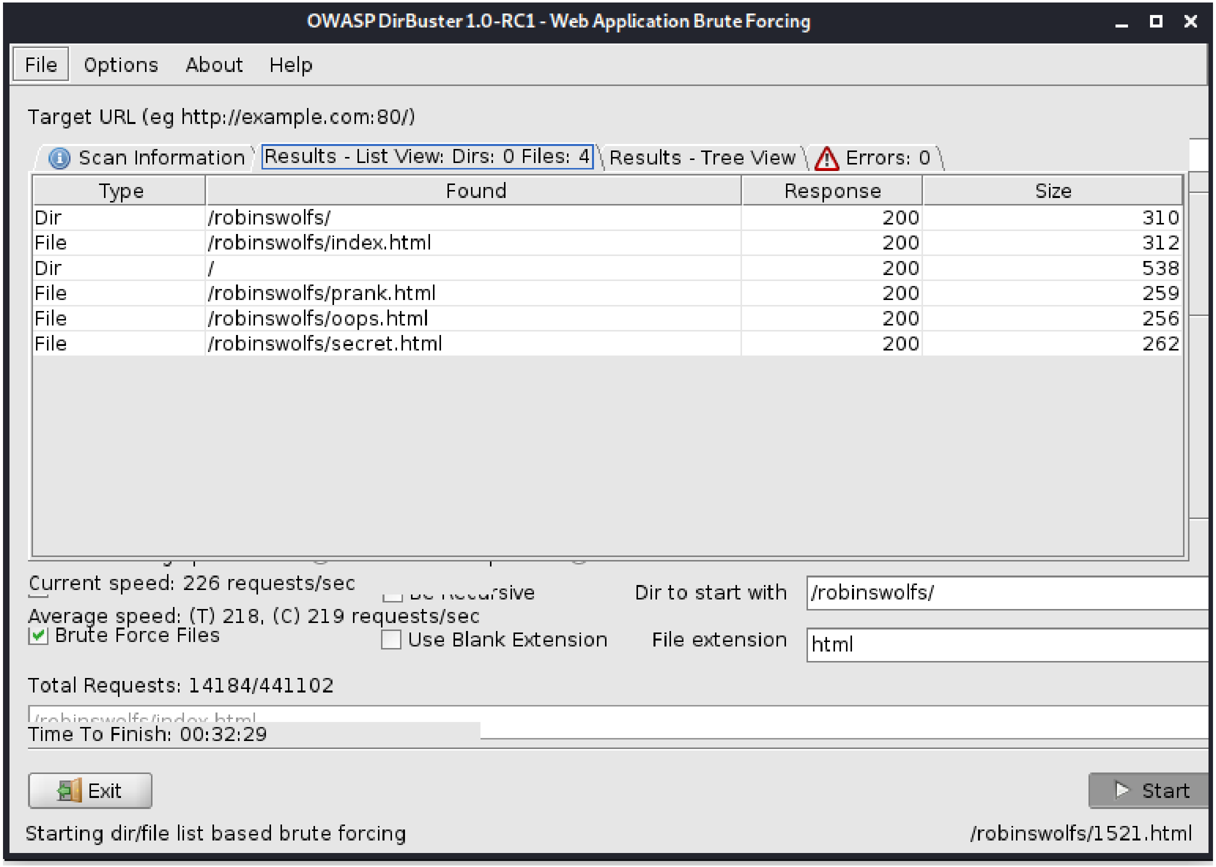
Total Requests: 3673/441102

Time To Finish: 00:34:52

Starting dir/file list based brute forcing /robinswolfs/phentermine.html

In the list click on “Results – List view: … “

After a minute or 2, this is the result:


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Scan Information
Results - List View: Dirs: 0 Files: 4
Results - Tree View
Errors: 0
Exit
Start

Target URL (eg http://example.com:80/)

Type	Found	Response	Size
Dir	/robinswolfs/	200	310
File	/robinswolfs/index.html	200	312
Dir	/	200	538
File	/robinswolfs/prank.html	200	259
File	/robinswolfs/oops.html	200	256
File	/robinswolfs/secret.html	200	262

Current speed: 226 requests/sec

Average speed: (T) 218, (C) 219 requests/sec

☑ Brute Force Files

□ Use Blank Extension

Dir to start with /robinswolfs/

File extension html

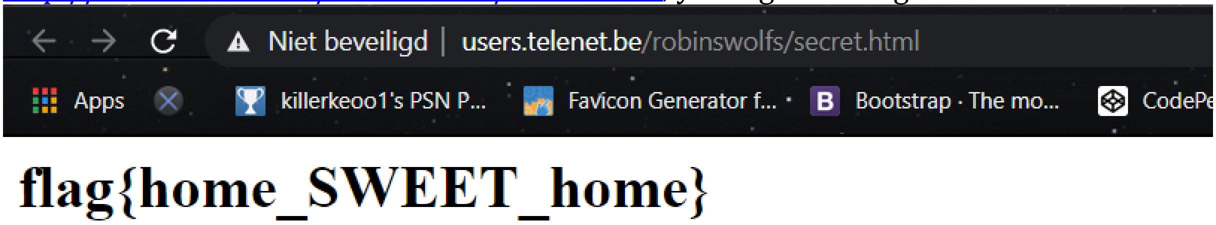
Total Requests: 14184/441102

Time To Finish: 00:32:29

Starting dir/file list based brute forcing /robinswolfs/1521.html

Apparently, there’s a secret.html file.

If you go to this site:
http://users.telenet.be/robinswolfs/secret.html, you'll get the flag.



flag{home_SWEET_home}

PART 3: The making of

The idea

I got inspiration from the sinners ctf. I had to use gimp to reposition some images, and I was so proud when I completed that challenge. So of course, I wanted to do something similar. But of course, I added a little twist towards the end.

The making of...

I simply created a GIMP file and started creating the small room. I added some layers with different attributes on the picture like a table, a door and a window.
Then I started making the little website. I hid the flag in a html file, which you can only find when you're using dirbuster.
Afterwards I made a QR code with the link of my site and put them behind the door.
In other words, you'll need to take a couple of steps before you can find the flag.

Troubleshooting

First I tried if I could find out if dirbuster worked. You'll need to change some settings like search for a html file of course. After 2 minutes or so, dirbuster found the html file.
I also send the GIMP file to some of my friends. Some had a hard time with it. Another friend said you could just go towards my github (because the site was hosted through github) and you could found the flag there easily. Github pages only works with public repo's. So the last step was to remove to site to my Telenet webspace.