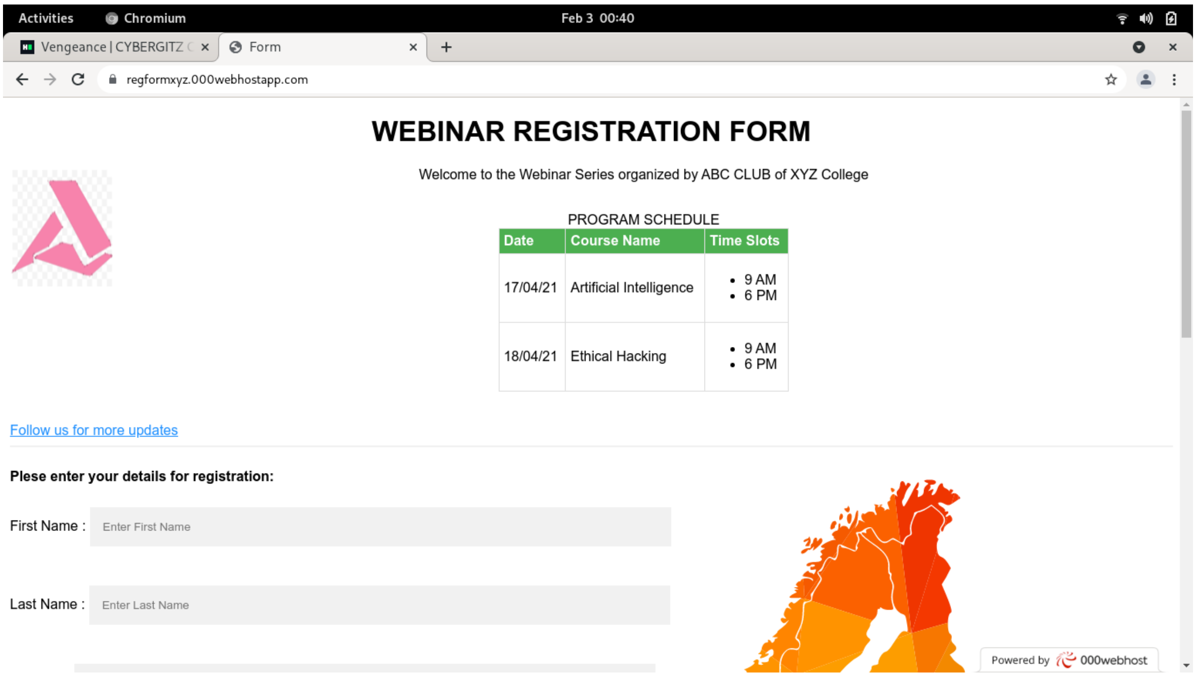
VENGEANCE.

This challenge also comes under the category of web exploitation except it's not a simple `robots.txt` file this time. There are actually some other hidden directories (or folders) inside it. To find them I used a tool known as DirBuster.



WEBINAR REGISTRATION FORM

Welcome to the Webinar Series organized by ABC CLUB of XYZ College

PROGRAM SCHEDULE

Date	Course Name	Time Slots
17/04/21	Artificial Intelligence	• 9 AM • 6 PM
18/04/21	Ethical Hacking	• 9 AM • 6 PM

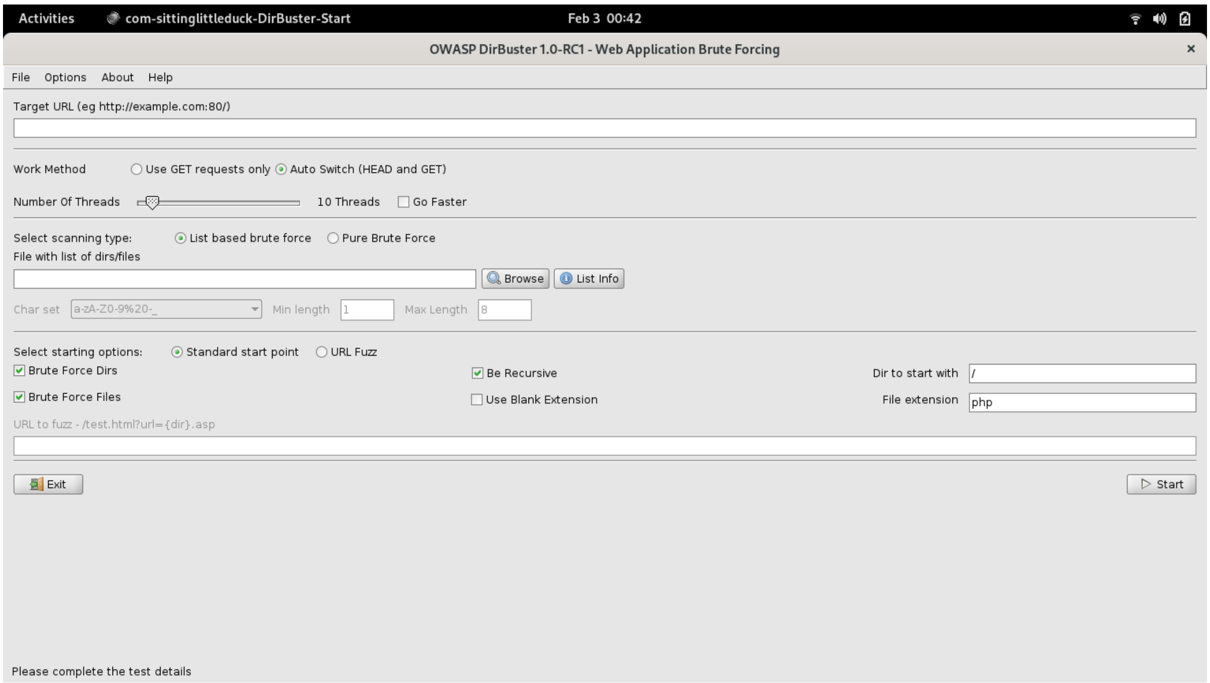
Follow us for more updates

Plese enter your details for registration:

First Name : Enter First Name

Last Name : Enter Last Name

This would be the main site and the following shown is the tool known as DirBuster.


Activities
com-sittinglittleduck-DirBuster-Start
Feb 3 00:42
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Browse
List Info
Exit
Start

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

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

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 /

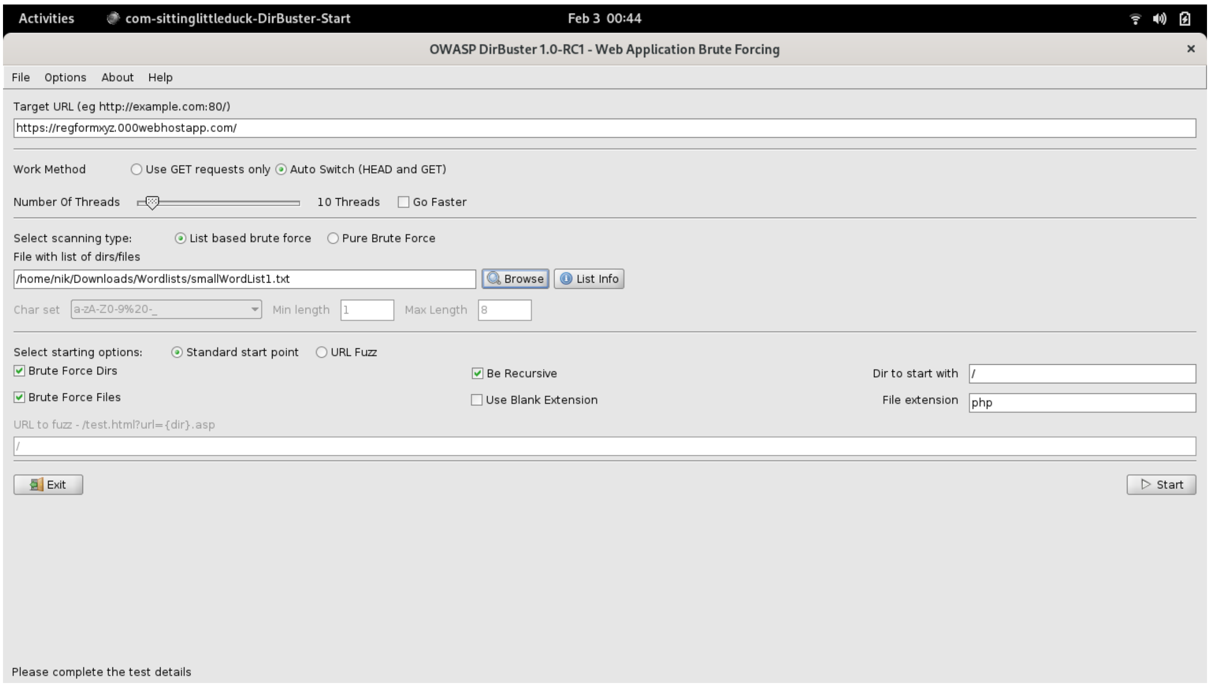
☑ Brute Force Files □ Use Blank Extension File extension php

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

Please complete the test details

It is a Java based application and hence you would need Java to be installed on your system as well.

The way this works is we give the target URL to the first field and a wordlist to the second field. We can change the other options according to our system but I won't be doing that here.



Activities
com-sittinglittleduck-DirBuster-Start
Feb 3 00:44
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Browse
List Info
Exit
Start

Target URL (eg http://example.com:80/)
https://regformxyz.000webhostapp.com/

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
/home/nik/Downloads/Wordlists/smallWordList1.txt

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

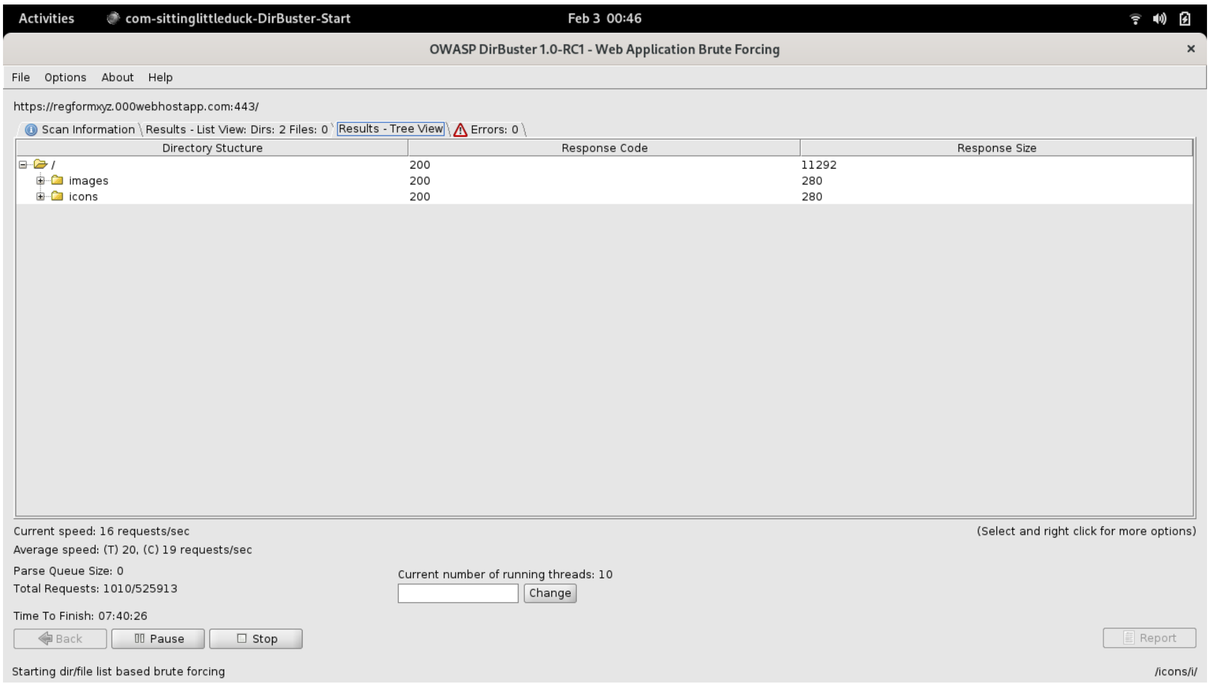
Select starting options: ● Standard start point ○ URL Fuzz

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

☑ Brute Force Files □ Use Blank Extension File extension php

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

Please complete the test details



Activities
com-sittinglittleduck-DirBuster-Start
Feb 3 00:46
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Scan Information
Results - List View: Dirs: 2 Files: 0
Results - Tree View
Errors: 0
Change
Back
Pause
Stop
Report

https://regformxyz.000webhostapp.com:443/

Directory Stucture	Response Code	Response Size
/	200	11292
images	200	280
icons	200	280

Current speed: 16 requests/sec
Average speed: (T) 20, (C) 19 requests/sec
Parse Queue Size: 0
Total Requests: 1010/525913
Time To Finish: 07:40:26

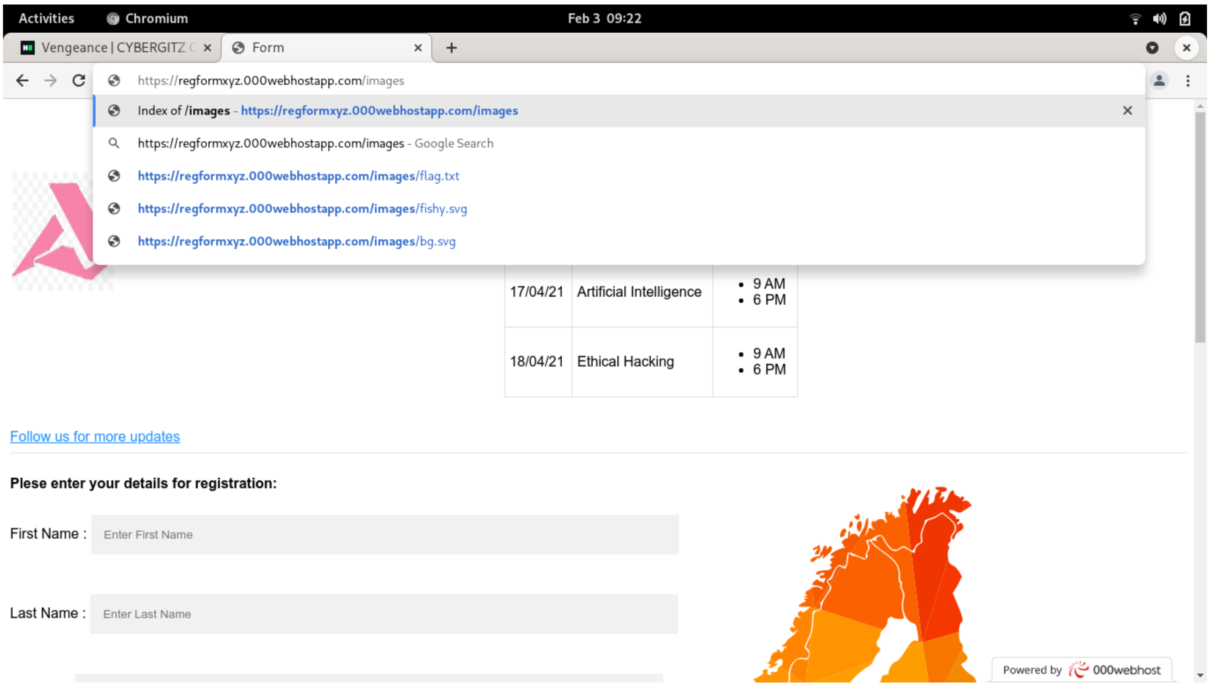
(Select and right click for more options)

Current number of running threads: 10

Starting dir/file list based brute forcing

/icons/i/

From the `Results- view tree tab` we can see that there are two directories - `images` and **`icons`** inside the main URL. Adding one of them (in this case **`images`**) to the main URL like so:



https://regformxyz.000webhostapp.com/images

Index of /images - https://regformxyz.000webhostapp.com/images

https://regformxyz.000webhostapp.com/images - Google Search

https://regformxyz.000webhostapp.com/images/flag.txt

https://regformxyz.000webhostapp.com/images/fishy.svg

https://regformxyz.000webhostapp.com/images/bg.svg

17/04/21	Artificial Intelligence	• 9 AM • 6 PM
18/04/21	Ethical Hacking	• 9 AM • 6 PM

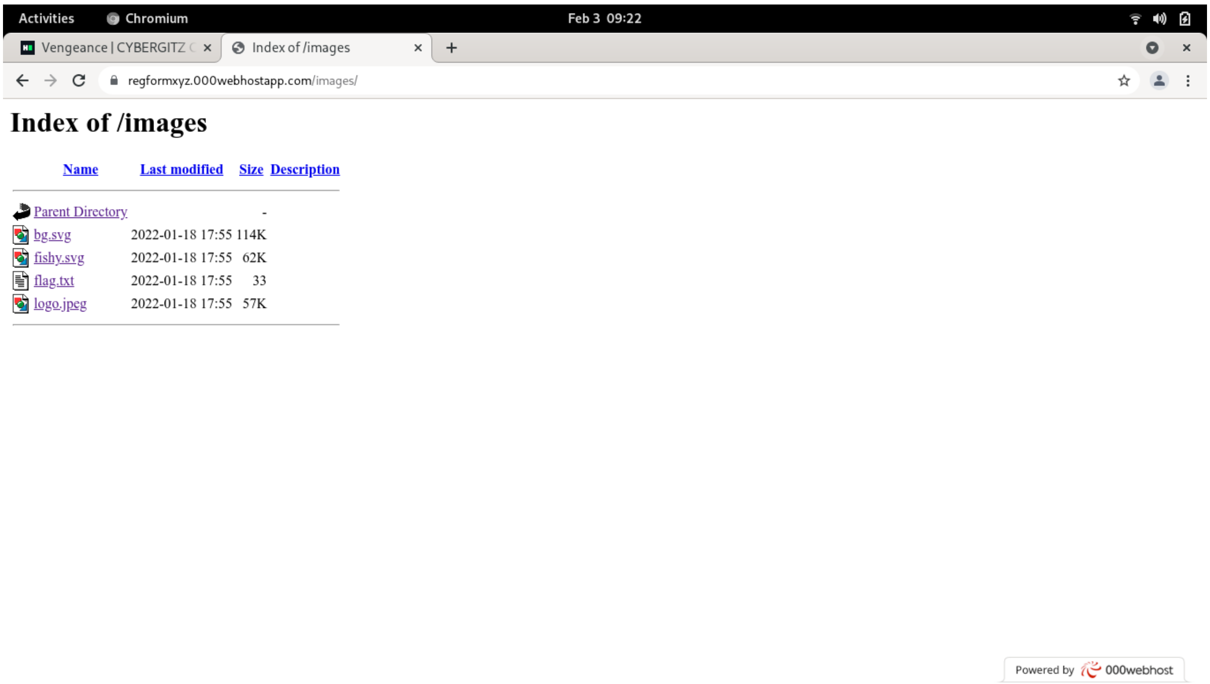
Follow us for more updates

Plese enter your details for registration:

First Name : Enter First Name

Last Name : Enter Last Name

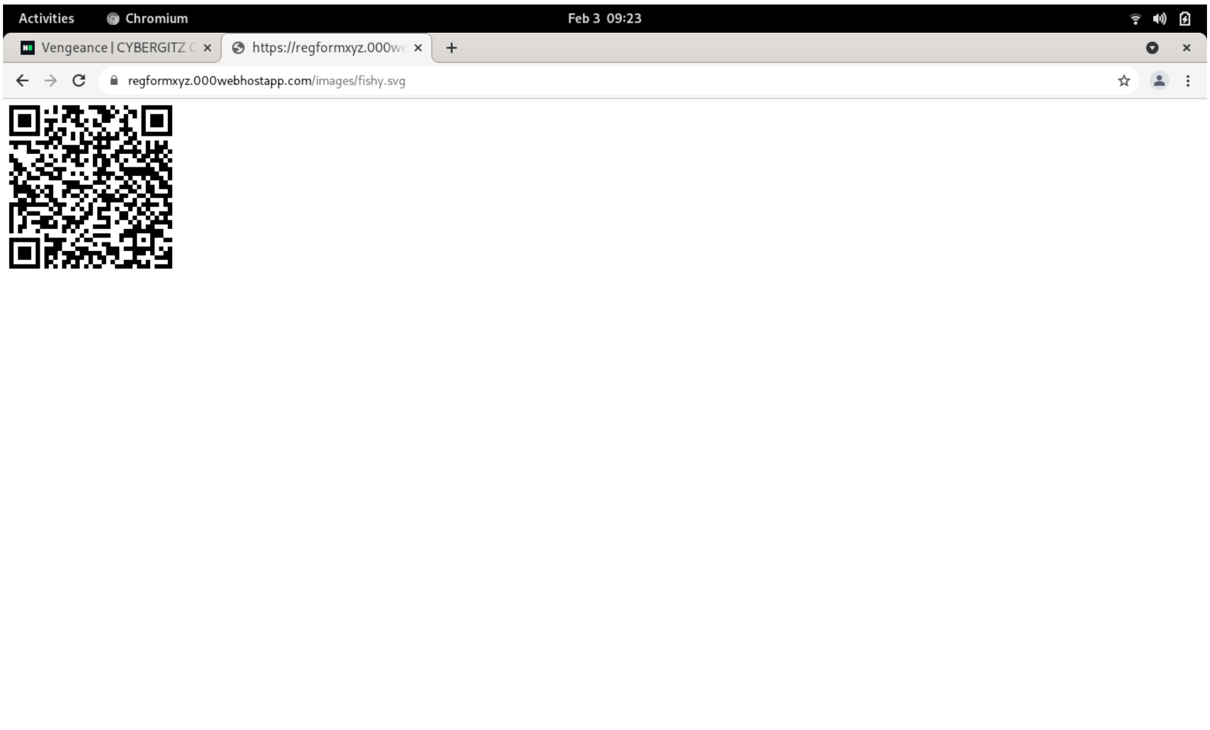
Take us to this page:



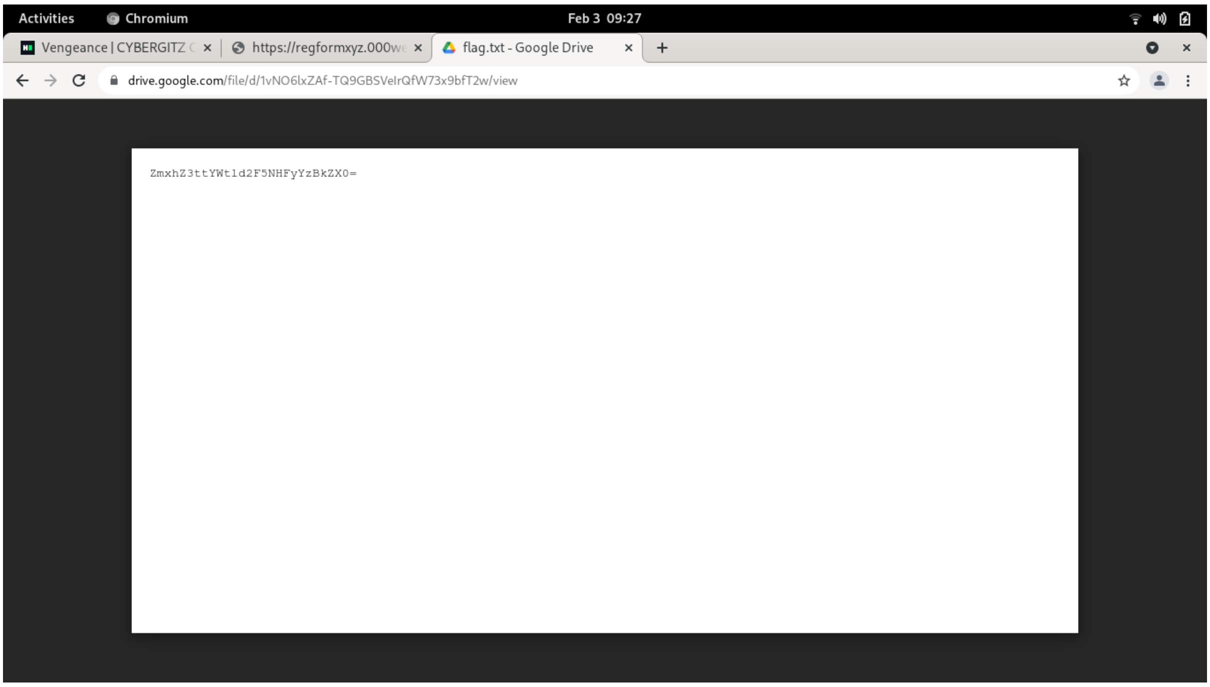
Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
bg.svg	2022-01-18 17:55	114K	
fishy.svg	2022-01-18 17:55	62K	
flag.txt	2022-01-18 17:55	33	
logo.jpeg	2022-01-18 17:55	57K	

Next step is to go through the files in that specific directory.

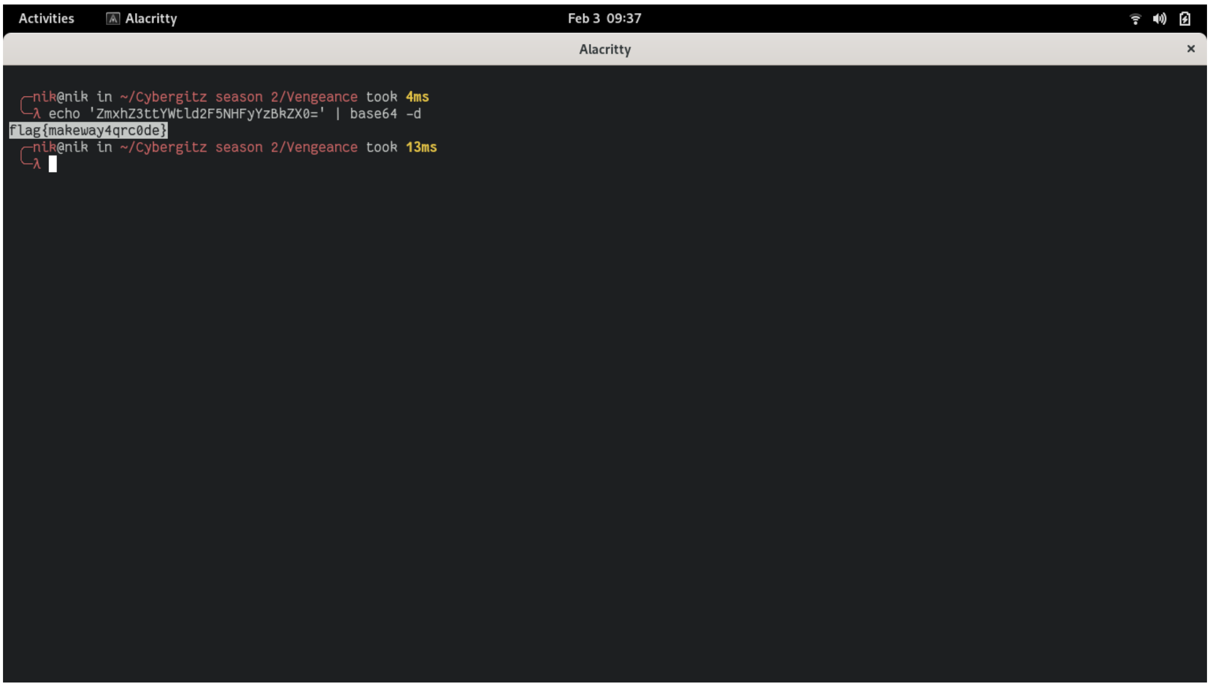


On opening this **`fishy.svg`** file we get this QR code. On scanning it we get the following:



```
ZmxhZ3ttYWtld2F5NHFyYzBkZX0=
```

Seems like a base64 so let’s decode it.



```
╭─nik@nik in ~/Cybergitz season 2/Vengeance took 4ms
╰─λ echo 'ZmxhZ3ttYWtld2F5NHFyYzBkZX0=' | base64 -d
flag{makeway4qrc0de}
╭─nik@nik in ~/Cybergitz season 2/Vengeance took 13ms
╰─λ
```

The highlighted text is the required flag.