TryHackMe - Corridor

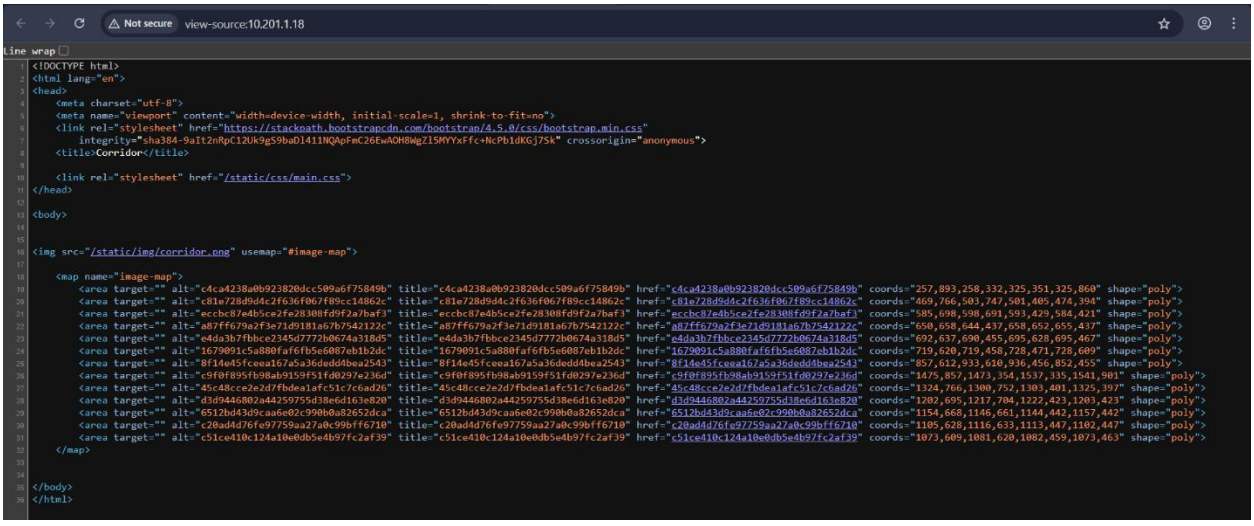
Question:

“ You have found yourself in a strange corridor. Can you find your way back to where you came from?

In this challenge, you will explore potential IDOR vulnerabilities. Examine the URL endpoints you access as you navigate the website and note the hexadecimal values you find (they look an awful lot like a *hash*, don’t they?). This could help you uncover website locations you were not expected to access.”

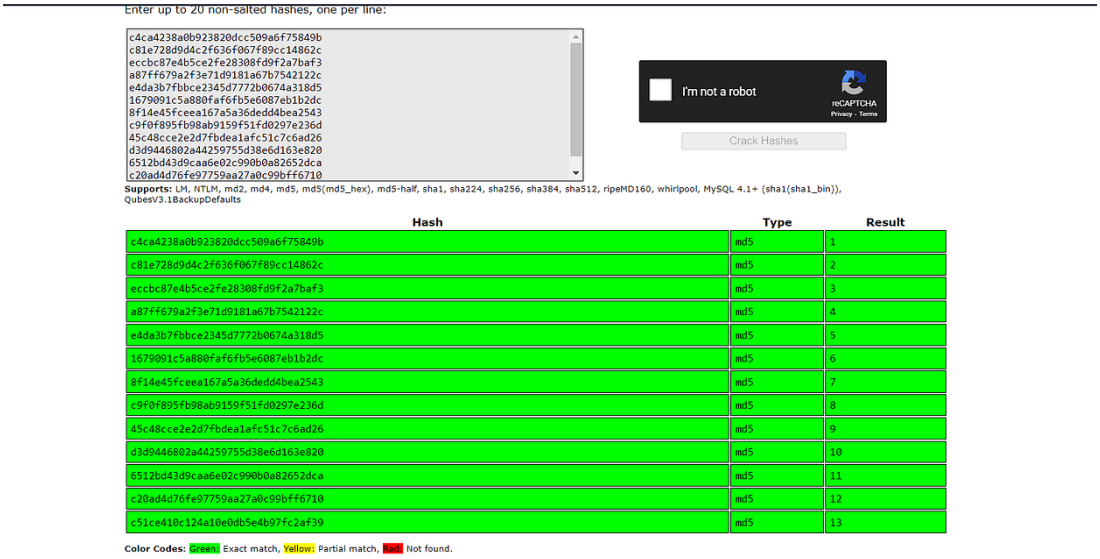
Machine IP

We noticed each door has a door number and when clicked gets directed to a webpage with a URL — http://IP/<md5-value-of-the-door-number>. so, by go into its Source Code, we got the list of the 13 doors.



Source Code Review

These numbers look quite suspicious so we decide to look into them using a CrackStation.



Enter up to 20 non-salted hashes, one per line:

```
c4ca4238a0b923820dcc509a6f75849b
c81e728d9d4c2f636f067f89cc14862c
eccbc87e4b5ce2fe28308fd9f2a7baf3
a87ff679a2f3e71d9181a67b7542122c
e4da3b7fbbce2345d7772b0674a318d5
1679091c5a880faf6fb5e6087eb1b2dc
8f14e45fceea167a5a36dedd4bea2543
c9f0f895fb98ab9159f51fd0297e236d
45c48cce2e2d7fbdea1afc51c7c6ad26
d3d9446802a44259755d38e6d163e820
6512bd43d9caa6e02c990b0a82652dca
c20ad4d76fe97759aa27a0c99bff6710
```

I'm not a robot — reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

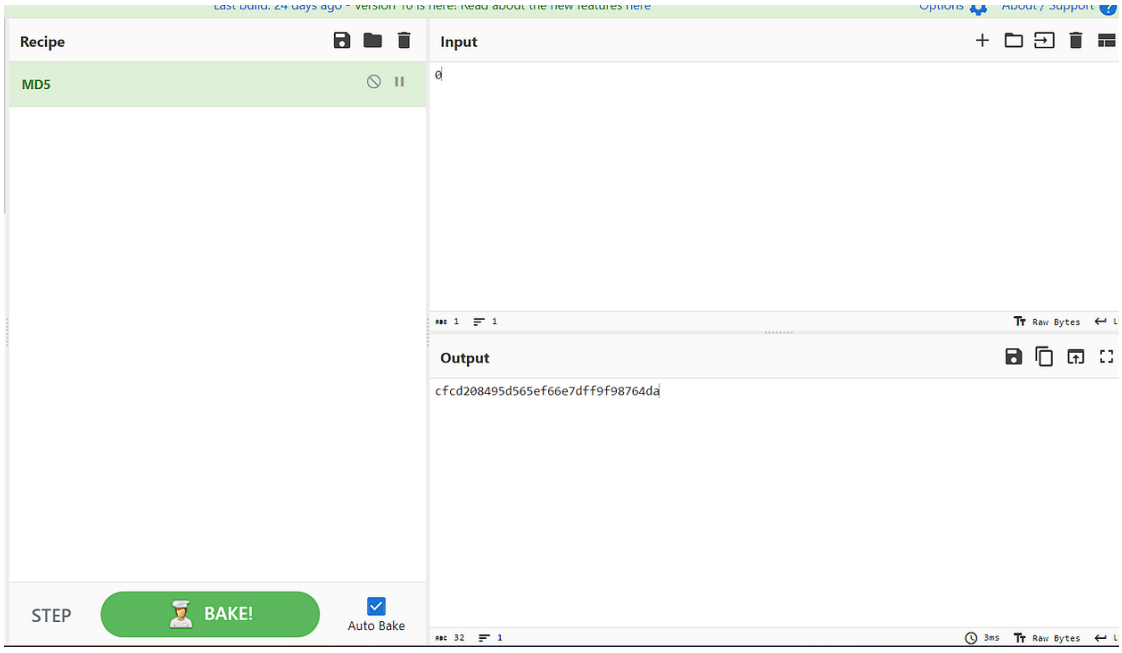
Hash	Type	Result
c4ca4238a0b923820dcc509a6f75849b	md5	1
c81e728d9d4c2f636f067f89cc14862c	md5	2
eccbc87e4b5ce2fe28308fd9f2a7baf3	md5	3
a87ff679a2f3e71d9181a67b7542122c	md5	4
e4da3b7fbbce2345d7772b0674a318d5	md5	5
1679091c5a880faf6fb5e6087eb1b2dc	md5	6
8f14e45fceea167a5a36dedd4bea2543	md5	7
c9f0f895fb98ab9159f51fd0297e236d	md5	8
45c48cce2e2d7fbdea1afc51c7c6ad26	md5	9
d3d9446802a44259755d38e6d163e820	md5	10
6512bd43d9caa6e02c990b0a82652dca	md5	11
c20ad4d76fe97759aa27a0c99bff6710	md5	12
c51ce410c124a10e0db5e4b97fc2af39	md5	13

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

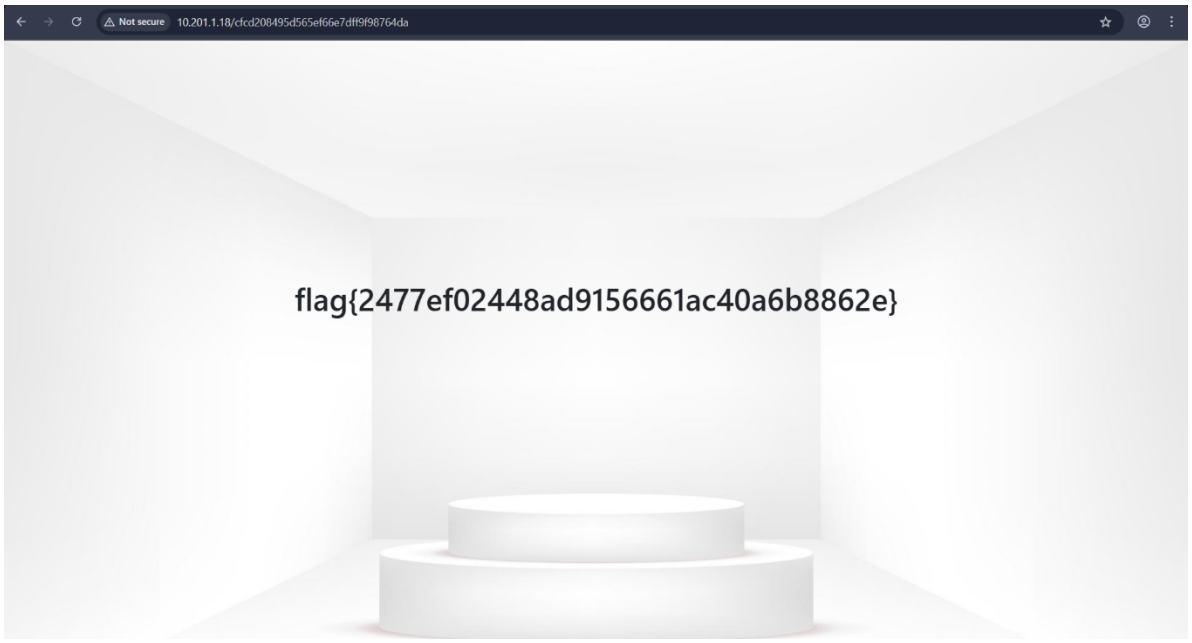
Using CrackStation to identify & crack the hashes

It appears the numbers is actually in md5 cipher and the result show a number from 1 to 13, which indicate door 1 until, but it seems missing a door number 0, so we decide to find the value of it.



Hash Value For 0 using CyberChef

Then we take the hash 0 value and paste it at the back of the Machine IP to open the door number 0, and finally we found the flag.



Flag Found