TryHackMe Room Write-up

Title: Corridor

Description: Can you escape the Corridor?

Author: Igor Buszta

Escape the Corridor

Description: *You have found yourself in a strange corridor. Can you find your way back to where you came?*

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.

Objective: What is the flag?

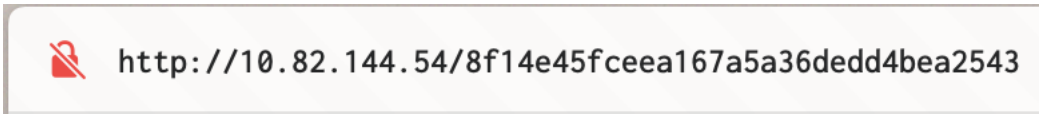
Tools: macOS, hash crackers.

We get a few hints at the beginning. The IDOR vulnerability (Insecure Direct Object Reference) is basically manipulating the URL to get into directories or change values to get restricted access.

There's also a hint that we should look at HEX values. We know where to start, let's investigate.

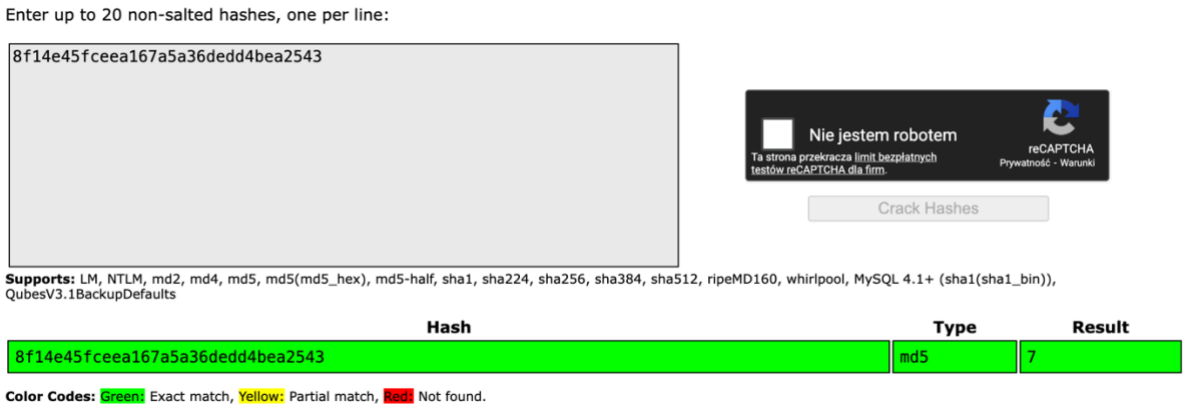
Picture 1: Front page.

The doors hide links to another sites. Let's click on the front one and see what's inside.



Picture 2: URL of the middle door.

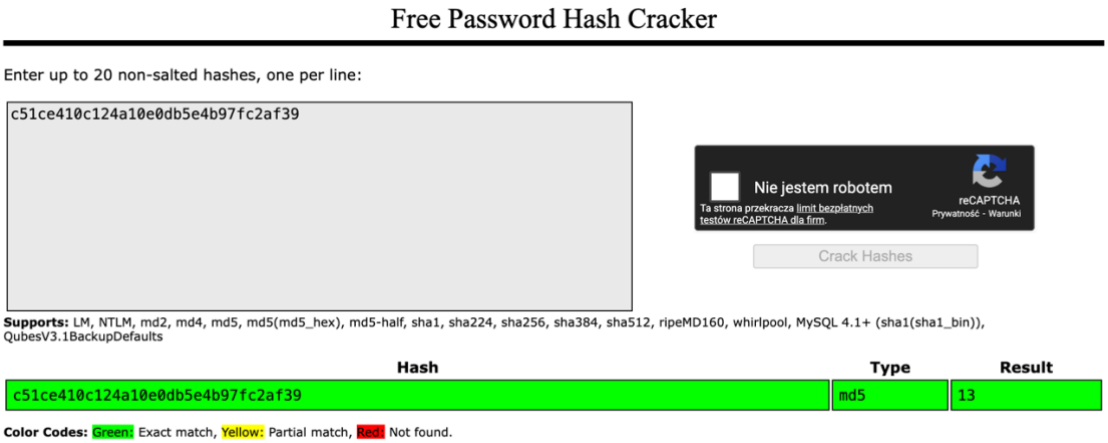
We already were hinted, that it might be a hash. You can use hashcat to crack it or online cracker.



Picture 3: Cracked hash from URL.

We are given number 7 as anwser. It should be a hint to something. Let's try a door to the right of the middle one.

Picture 4: URL of another door.

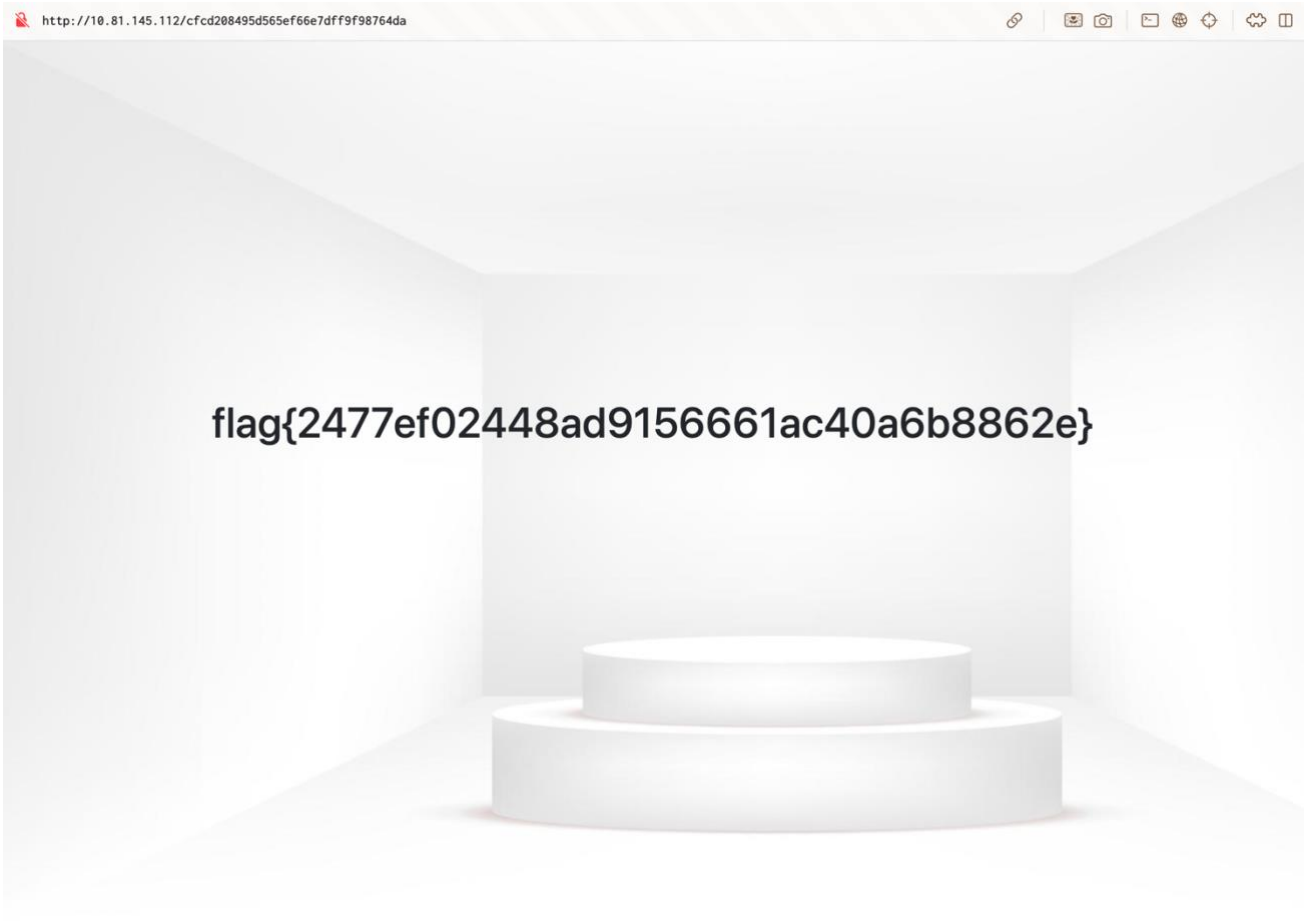


Picture 5: Another cracked hash from URL.

This one is marked as 13. There are 13 doors in total, so we can assume that all the hashes represent a number. Following that trail, the task is to escape this corridor, even to go back from there. We should try to generate a MD5 hash of number 0 and enter the given hash into URL.

```
> echo -n 0 > 0.txt
> md5sum 0.txt
cfcd208495d565ef66e7dff9f98764da  0.txt
>
```

Picture 6: Generating MD5 hash of number 0.



Picture 7: Result of entering our hash into URL.

Job is done.