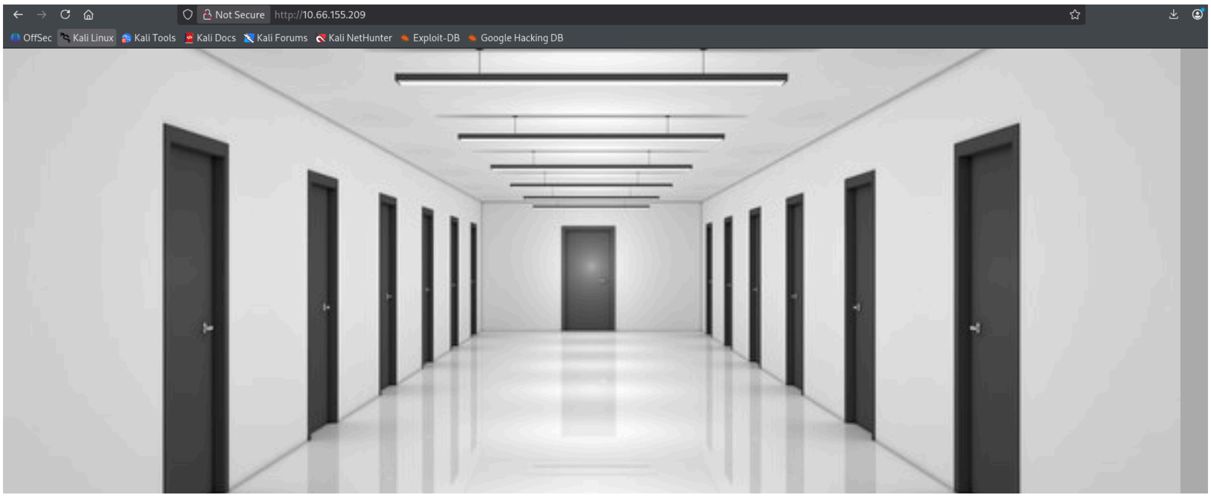
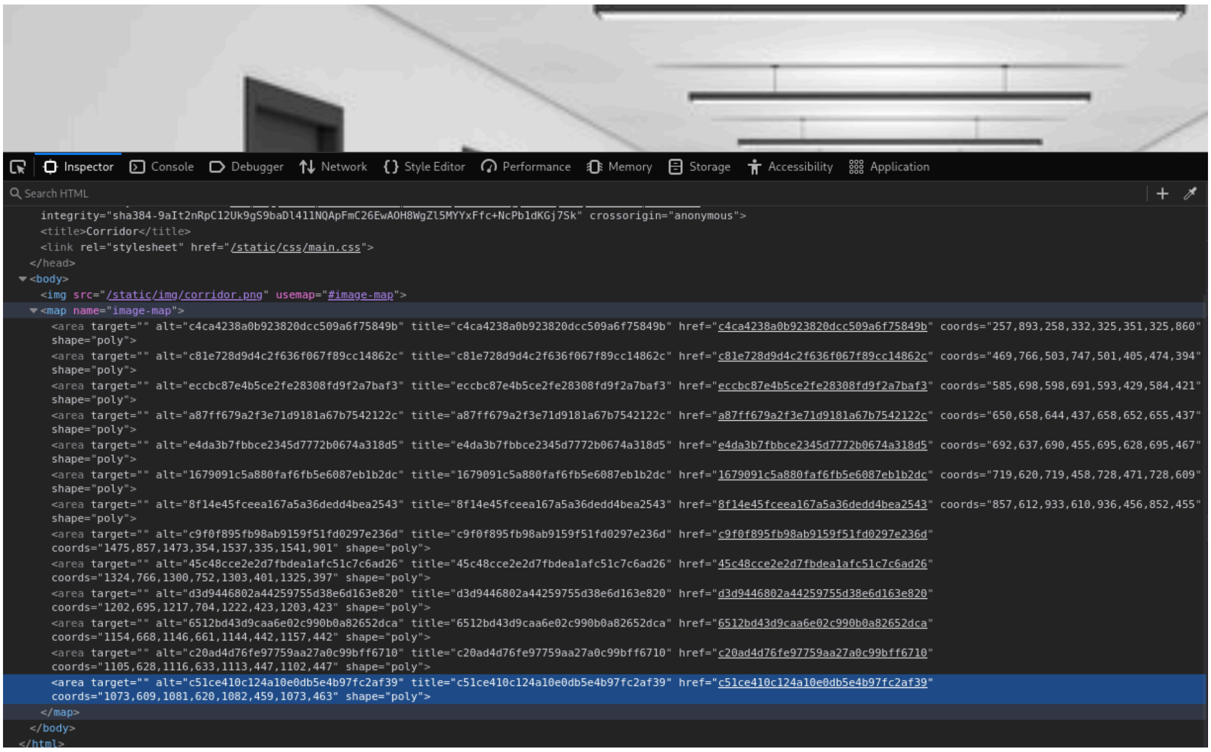
Corridor

ip: 10.66.155.209

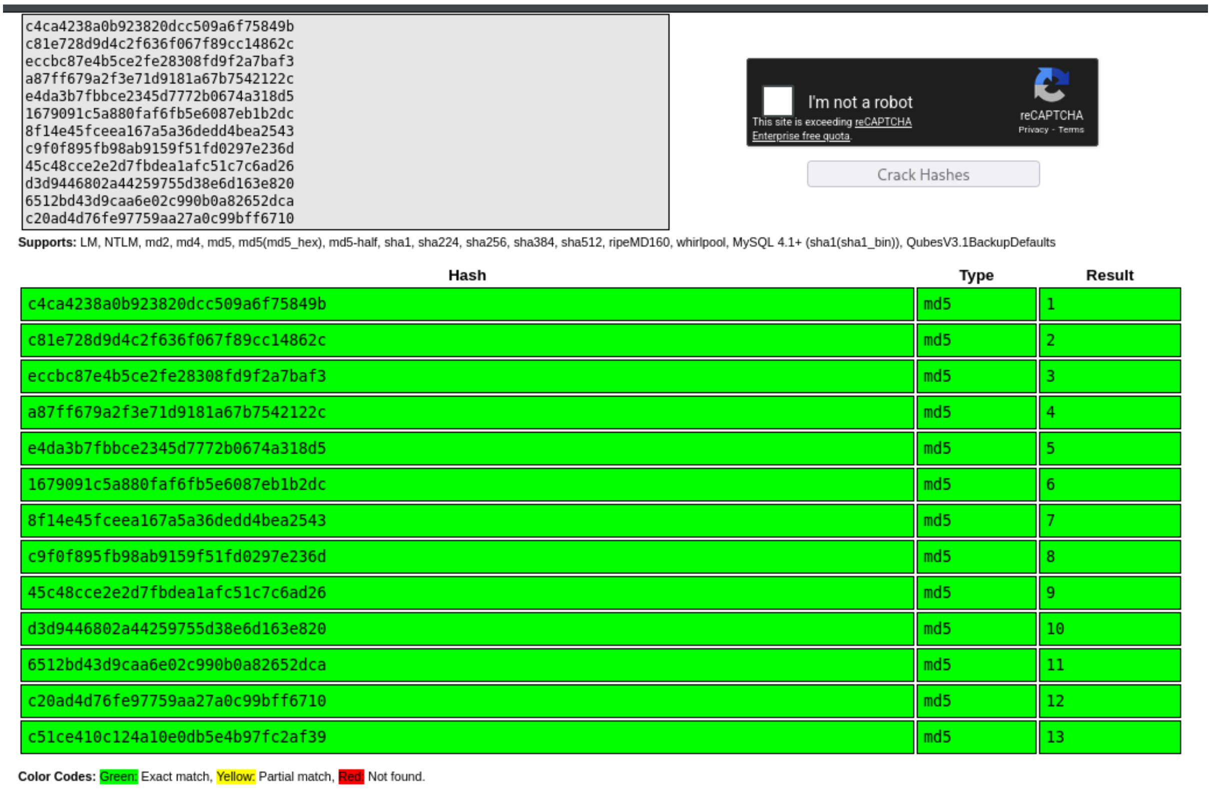


```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 61 Werkzeug httpd 2.0.3 (Python 3.10.2)
| http-methods: 
|_  Supported Methods: OPTIONS HEAD GET
|_http-title: Corridor
```



```
    integrity="sha384-9aIt2nRpC12Uk9gS9baDl411NQApFmC26EwAOH8WgZl5MYYxFfc+NcPb1dKGj7Sk" crossorigin="anonymous">
    <title>Corridor</title>
    <link rel="stylesheet" href="/static/css/main.css">
  </head>
▼ <body>
    <img src="/static/img/corridor.png" usemap="#image-map">
  ▼ <map name="image-map">
      <area target="" alt="c4ca4238a0b923820dcc509a6f75849b" title="c4ca4238a0b923820dcc509a6f75849b" href="c4ca4238a0b923820dcc509a6f75849b" coords="257,893,258,332,325,351,325,860"
      shape="poly">
      <area target="" alt="c81e728d9d4c2f636f067f89cc14862c" title="c81e728d9d4c2f636f067f89cc14862c" href="c81e728d9d4c2f636f067f89cc14862c" coords="469,766,503,747,501,405,474,394"
      shape="poly">
      <area target="" alt="eccbc87e4b5ce2fe28308fd9f2a7baf3" title="eccbc87e4b5ce2fe28308fd9f2a7baf3" href="eccbc87e4b5ce2fe28308fd9f2a7baf3" coords="585,698,598,691,593,429,584,421"
      shape="poly">
      <area target="" alt="a87ff679a2f3e71d9181a67b7542122c" title="a87ff679a2f3e71d9181a67b7542122c" href="a87ff679a2f3e71d9181a67b7542122c" coords="650,658,644,437,658,652,655,437"
      shape="poly">
      <area target="" alt="e4da3b7fbbce2345d7772b0674a318d5" title="e4da3b7fbbce2345d7772b0674a318d5" href="e4da3b7fbbce2345d7772b0674a318d5" coords="692,637,690,455,695,628,695,467"
      shape="poly">
      <area target="" alt="1679091c5a880faf6fb5e6087eb1b2dc" title="1679091c5a880faf6fb5e6087eb1b2dc" href="1679091c5a880faf6fb5e6087eb1b2dc" coords="719,620,719,458,728,471,728,609"
      shape="poly">
      <area target="" alt="8f14e45fceea167a5a36dedd4bea2543" title="8f14e45fceea167a5a36dedd4bea2543" href="8f14e45fceea167a5a36dedd4bea2543" coords="857,612,933,610,936,456,852,455"
      shape="poly">
      <area target="" alt="c9f0f895fb98ab9159f51fd0297e236d" title="c9f0f895fb98ab9159f51fd0297e236d" href="c9f0f895fb98ab9159f51fd0297e236d"
      coords="1475,857,1473,354,1537,335,1541,901" shape="poly">
      <area target="" alt="45c48cce2e2d7fbdea1afc51c7c6ad26" title="45c48cce2e2d7fbdea1afc51c7c6ad26" href="45c48cce2e2d7fbdea1afc51c7c6ad26"
      coords="1324,766,1300,752,1303,401,1325,397" shape="poly">
      <area target="" alt="d3d9446802a44259755d38e6d163e820" title="d3d9446802a44259755d38e6d163e820" href="d3d9446802a44259755d38e6d163e820"
      coords="1202,695,1217,704,1222,423,1203,423" shape="poly">
      <area target="" alt="6512bd43d9caa6e02c990b0a82652dca" title="6512bd43d9caa6e02c990b0a82652dca" href="6512bd43d9caa6e02c990b0a82652dca"
      coords="1154,668,1146,661,1144,442,1157,442" shape="poly">
      <area target="" alt="c20ad4d76fe97759aa27a0c99bff6710" title="c20ad4d76fe97759aa27a0c99bff6710" href="c20ad4d76fe97759aa27a0c99bff6710"
      coords="1105,628,1116,633,1113,447,1102,447" shape="poly">
      <area target="" alt="c51ce410c124a10e0db5e4b97fc2af39" title="c51ce410c124a10e0db5e4b97fc2af39" href="c51ce410c124a10e0db5e4b97fc2af39"
      coords="1073,609,1081,620,1082,459,1073,463" shape="poly">
    </map>
  </body>
</html>
```

https://crackstation.net/



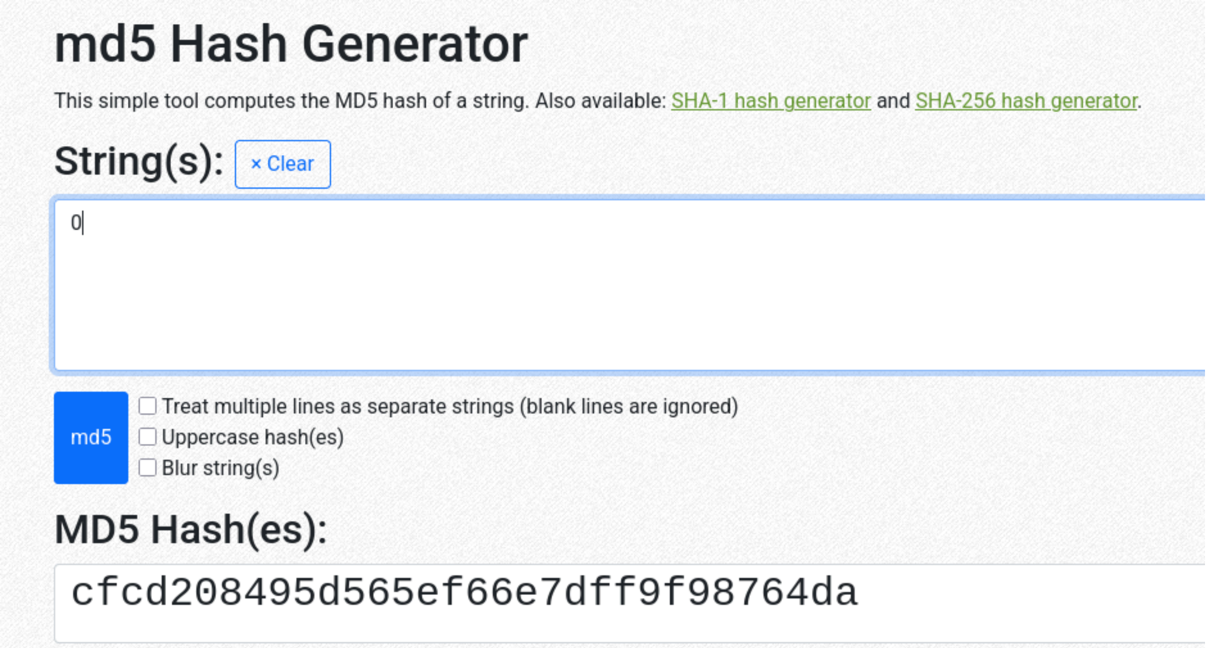
```
c4ca4238a0b923820dcc509a6f75849b
c81e728d9d4c2f636f067f89cc14862c
eccbc87e4b5ce2fe28308fd9f2a7baf3
a87ff679a2f3e71d9181a67b7542122c
e4da3b7fbbce2345d7772b0674a318d5
1679091c5a880faf6fb5e6087eb1b2dc
8f14e45fceea167a5a36dedd4bea2543
c9f0f895fb98ab9159f51fd0297e236d
45c48cce2e2d7fbdea1afc51c7c6ad26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

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.

https://www.miraclesalad.com/webtools/md5.php



md5 Hash Generator

This simple tool computes the MD5 hash of a string. Also available: SHA-1 hash generator and SHA-256 hash generator.

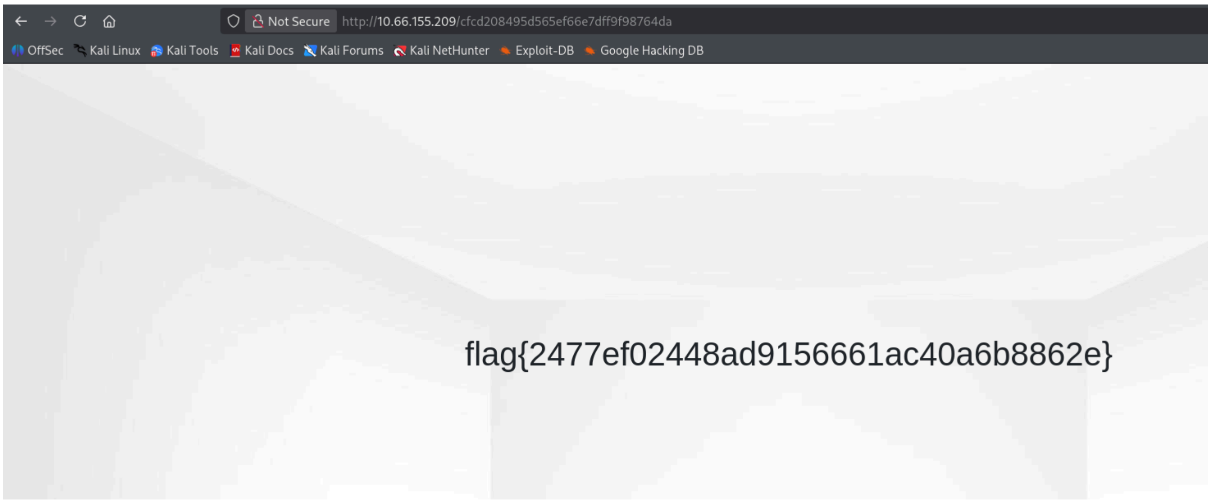
String(s): × Clear

```
0
```

☐ Treat multiple lines as separate strings (blank lines are ignored)
☐ Uppercase hash(es)
☐ Blur string(s)

MD5 Hash(es):

```
cfcd208495d565ef66e7dff9f98764da
```

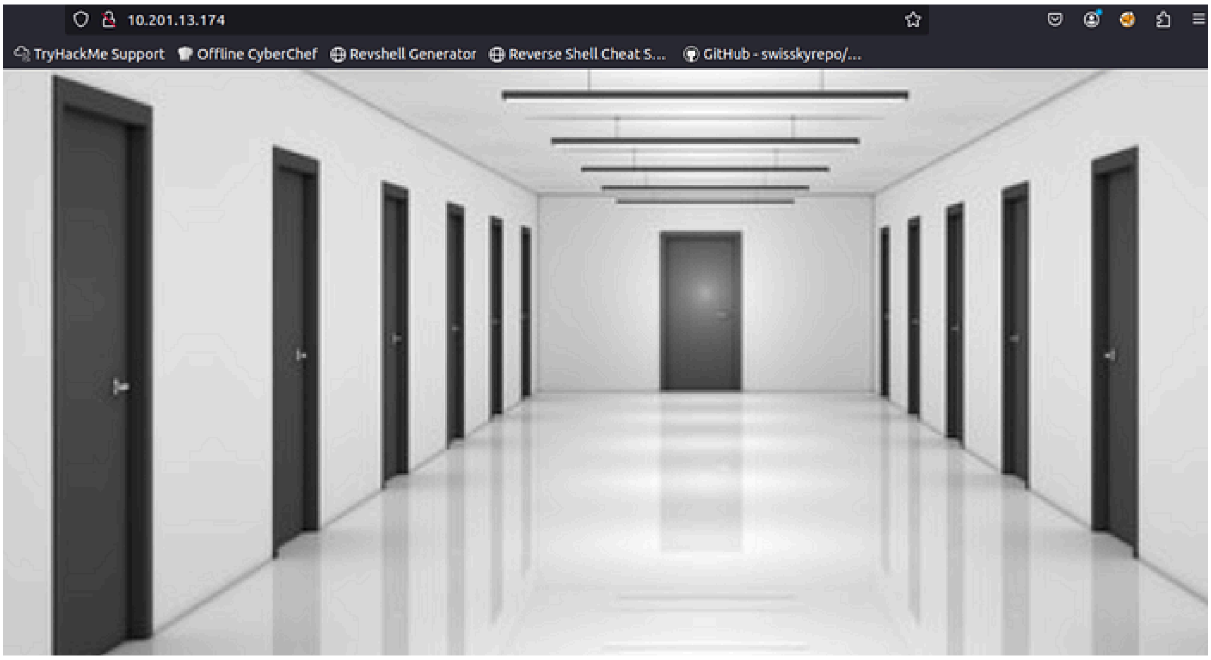


flag{2477ef02448ad9156661ac40a6b8862e}

investigate possible IDOR (Insecure Direct Object Reference) vulnerabilities by examining the hexadecimal values in the URLs. We may also need to try to access different resources or user data by manipulating these values to reach pages that we are not authorized to access.

Visiting the website, we find a lot of doors, all of which are clickable:

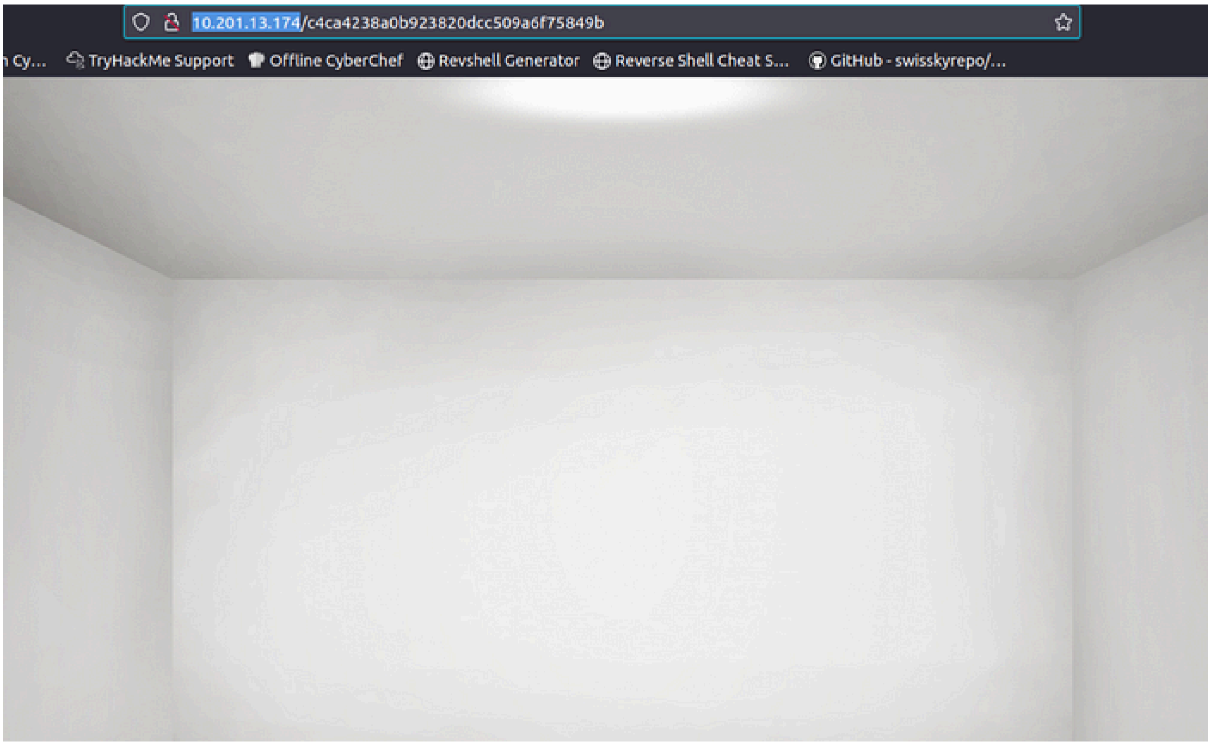
Press enter or click to view image in full size



13 doors click able

There are 13 doors that we can see here. When we click on any of them, we see an empty room:

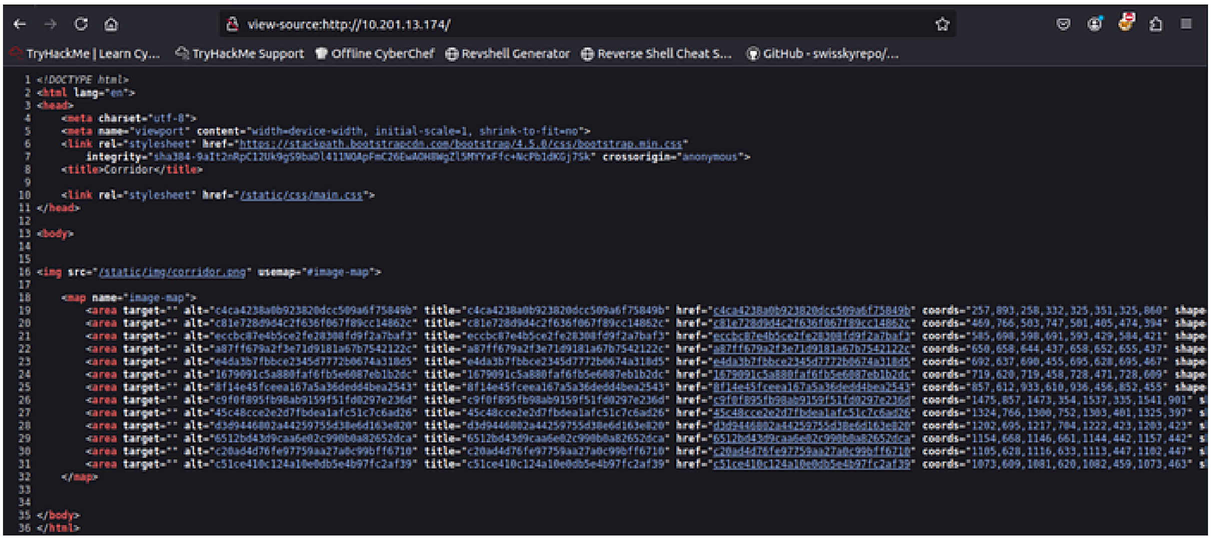
Press enter or click to view image in full size



Empty Room

When we look at the page codes, we see 13 links that are compatible with the image:

Press enter or click to view image in full size

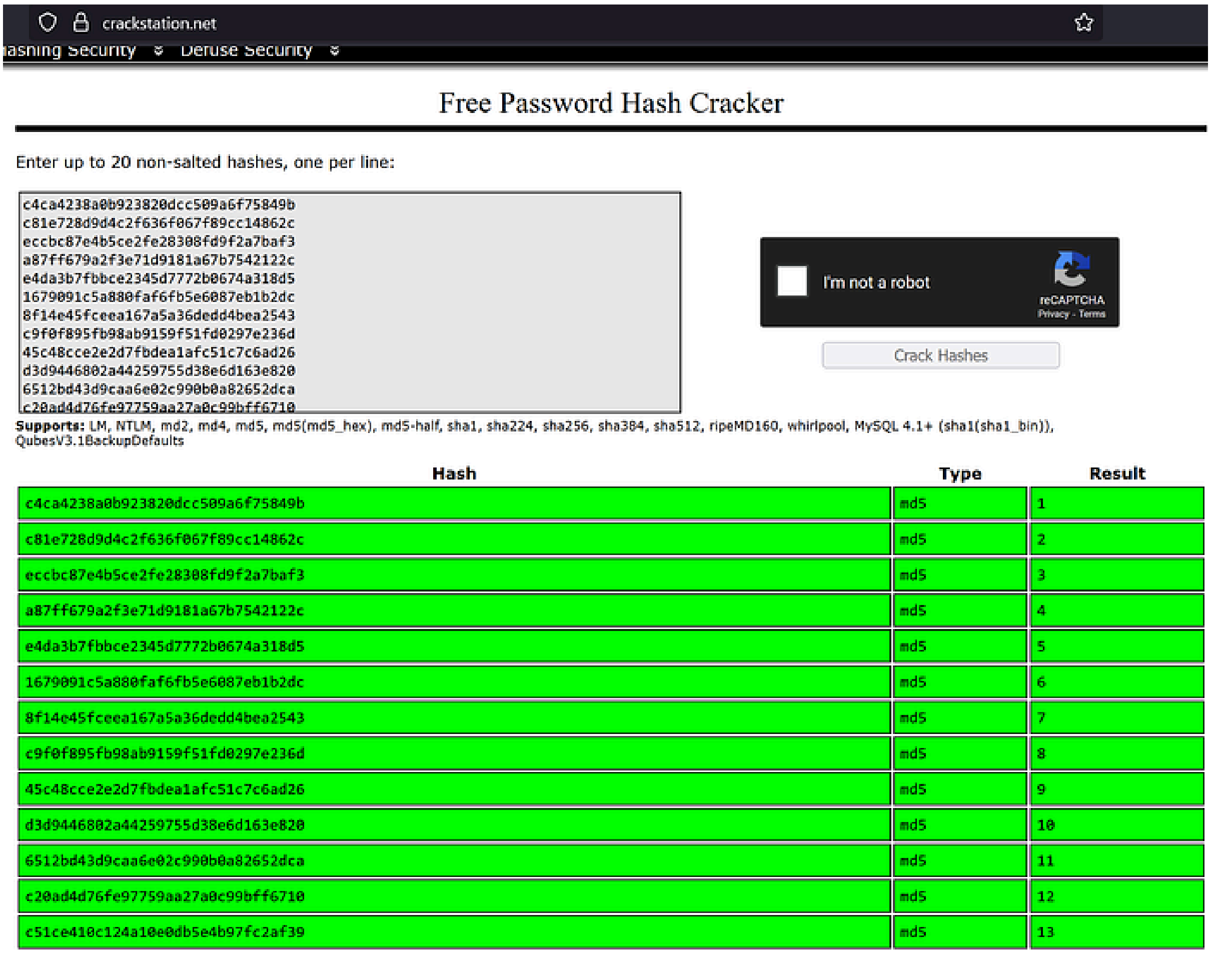


```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css"
        integrity="sha384-9aIt2nRpC12Uk9gS9baDl411NQApFmC26EwAOH8WgZl5MYYxFfc+NcPb1dKGj7Sk" crossorigin="anonymous">
    <title>Corridor</title>

    <link rel="stylesheet" href="/static/css/main.css">
</head>

<body>


<img src="/static/img/corridor.png" usemap="#image-map">

    <map name="image-map">
        <area target="" alt="c4ca4238a0b923820dcc509a6f75849b" title="c4ca4238a0b923820dcc509a6f75849b" href="c4ca4238a0b923820dcc509a6f75849b" coords="257,893,258,332,325,351,325,860" shape
        <area target="" alt="c81e728d9d4c2f636f067f89cc14862c" title="c81e728d9d4c2f636f067f89cc14862c" href="c81e728d9d4c2f636f067f89cc14862c" coords="469,766,503,747,501,405,474,394" shape
        <area target="" alt="eccbc87e4b5ce2fe28308fd9f2a7baf3" title="eccbc87e4b5ce2fe28308fd9f2a7baf3" href="eccbc87e4b5ce2fe28308fd9f2a7baf3" coords="585,698,598,691,593,429,584,421" shape
        <area target="" alt="a87ff679a2f3e71d9181a67b7542122c" title="a87ff679a2f3e71d9181a67b7542122c" href="a87ff679a2f3e71d9181a67b7542122c" coords="650,658,644,437,658,652,655,437" shape
        <area target="" alt="e4da3b7fbbce2345d7772b0674a318d5" title="e4da3b7fbbce2345d7772b0674a318d5" href="e4da3b7fbbce2345d7772b0674a318d5" coords="692,637,690,455,695,628,695,467" shape
        <area target="" alt="1679091c5a880faf6fb5e6087eb1b2dc" title="1679091c5a880faf6fb5e6087eb1b2dc" href="1679091c5a880faf6fb5e6087eb1b2dc" coords="719,620,719,458,728,471,728,609" shape
        <area target="" alt="8f14e45fceea167a5a36dedd4bea2543" title="8f14e45fceea167a5a36dedd4bea2543" href="8f14e45fceea167a5a36dedd4bea2543" coords="857,612,933,610,936,456,852,455" shape
        <area target="" alt="c9f0f895fb98ab9159f51fd0297e236d" title="c9f0f895fb98ab9159f51fd0297e236d" href="c9f0f895fb98ab9159f51fd0297e236d" coords="1475,857,1473,354,1537,335,1541,901" s
        <area target="" alt="45c48cce2e2d7fbdea1afc51c7c6ad26" title="45c48cce2e2d7fbdea1afc51c7c6ad26" href="45c48cce2e2d7fbdea1afc51c7c6ad26" coords="1324,766,1300,752,1303,401,1325,397" s
        <area target="" alt="d3d9446802a44259755d38e6d163e820" title="d3d9446802a44259755d38e6d163e820" href="d3d9446802a44259755d38e6d163e820" coords="1202,695,1217,704,1222,423,1203,423" s
        <area target="" alt="6512bd43d9caa6e02c990b0a82652dca" title="6512bd43d9caa6e02c990b0a82652dca" href="6512bd43d9caa6e02c990b0a82652dca" coords="1154,668,1146,661,1144,442,1157,442" s
        <area target="" alt="c20ad4d76fe97759aa27a0c99bff6710" title="c20ad4d76fe97759aa27a0c99bff6710" href="c20ad4d76fe97759aa27a0c99bff6710" coords="1105,628,1116,633,1113,447,1102,447" s
        <area target="" alt="c51ce410c124a10e0db5e4b97fc2af39" title="c51ce410c124a10e0db5e4b97fc2af39" href="c51ce410c124a10e0db5e4b97fc2af39" coords="1073,609,1081,620,1082,459,1073,463" s
    </map>


</body>
</html>
```

The title, the page it points to and the alternative text of each link consist of a fixed and most likely encoded value. Most likely, when we decrypt this data, we will go to another link that does not have a link here and solve the CTF.

We see that each encrypted value consists of 32 characters. This reminds us of MD5. Now let’s convert the data in order, starting with MD5, which is the most probable encryption. You don’t have to do this with code or another script. You can quickly find a solution with https://crackstation.net/or any similar site.

Press enter or click to view image in full size



Free Password Hash Cracker

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

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

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

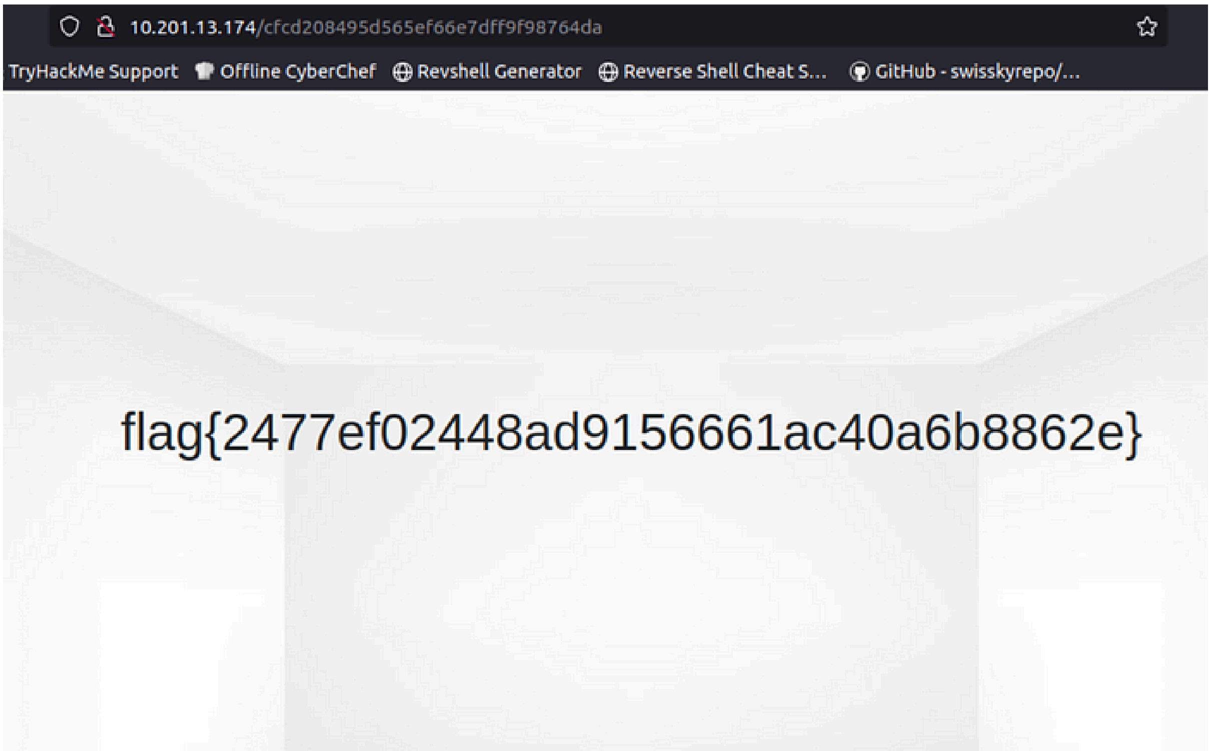
Hash	Type	Result
c4ca4238a0b923820dcc509a6f75849b	md5	1
c81e728d9d4c2f636f067f89cc14862c	md5	2
eccbc87e4b5ce2fe28308fd9f2a7baf3	md5	3
a87ff679a2f3e71d9181a67b7542122c	md5	4
e4da3b7fbbce2345d7772b0674a318d5	md5	5
1679091c5a880faf6fb5e6087eb1b2dc	md5	6
8f14e45fceea167a5a36dedd4bea2543	md5	7
c9f0f895fb98ab9159f51fd0297e236d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

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

If you notice, the MD5 hashes of the numbers from 1 to 13. If we are going to find an IDOR vulnerability, what we need to do is to get the MD5 hash values of the numbers starting from 0 and 14 and in a way “enter through invisible doors”. Now, let’s take the easy way out without dealing with code or script and add the hash value of each number to the site extension from https://www.miraclesalad.com/webtools/md5.php and open our site in the browser. Let’s get started:

0 → cfcd208495d565ef66e7dff9f98764da → http://TARGET_IP/cfcd208495d565ef66e7dff9f98764da

Press enter or click to view image in full size



10.201.13.174/cfcd208495d565ef66e7dff9f98764da

flag{2477ef02448ad9156661ac40a6b8862e}

flag{2477ef02448ad9156661ac40a6b8862e}

Insecure Direct Object Reference (IDOR) is a vulnerability that arises when attackers can access or modify objects by manipulating identifiers used in a web application's URLs or parameters. It occurs due to missing access control checks, which fail to verify whether a user should be allowed to access specific data.

What is the flag?

flag{2477ef02448ad9156661ac40a6b8862e}