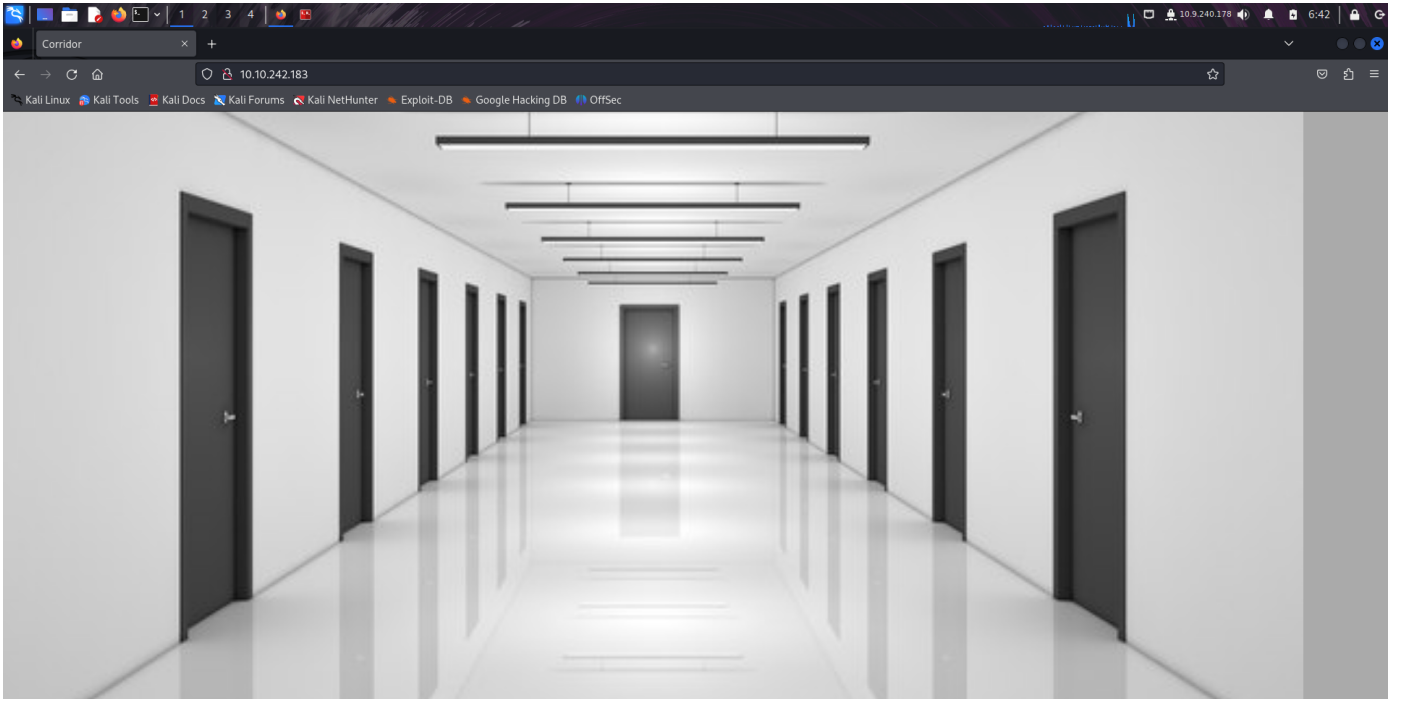
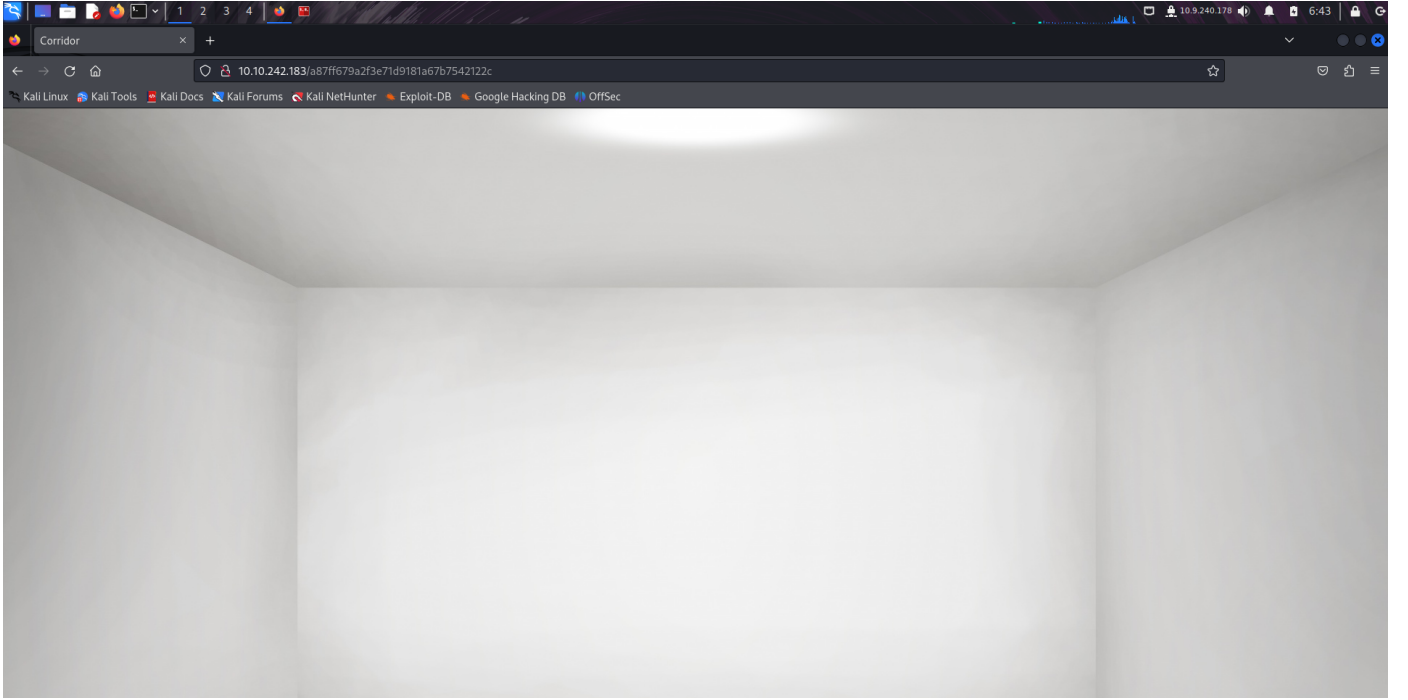


80 portunun açık olduğunu görüyoruz. Nmap taramasına 80 portu için şuanlık gerek yok.



Web sitesine girdiğimizde bizi böyle bir sayfa karşılıyor.



Kapılara tıkladığımızda ise bizi böyle boş odalara yönlendiriyor. Urlde bizi yönlendirdiği sub domain şifrelenmiş olarak gözüküyor

Sayfanın kaynak kodlarına baktığımızda ise

```
Corridor x http://10.10.242.183/ x +
view-source:http://10.10.242.183/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <meta charset="utf-8">
5 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
6 <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css"
7 integrity="sha384-9a12nMpC12UKg99b014110ApFmc26ewA0H8mgZ1SYYx7Ffc+NcPb1dKG7Sk" crossorigin="anonymous">
8 <title>Corridor</title>
9
10 <link rel="stylesheet" href="/static/css/main.css">
11 </head>
12
13 <body>
14
15
16 
17
18 <map name="image-map">
19 <area target="" alt="c4ca4238a0b923820dcc509a6f75849b" title="c4ca4238a0b923820dcc509a6f75849b" href="/c4ca4238a0b923820dcc509a6f75849b" coords="257,803,258,332,325,351,325,860" shape="poly">
20 <area target="" alt="c81e728d9d4c2f636f067f89cc14862c" title="c81e728d9d4c2f636f067f89cc14862c" href="/c81e728d9d4c2f636f067f89cc14862c" coords="469,766,503,747,501,405,474,394" shape="poly">
21 <area target="" alt="eccbc87e4b5ce2fe28308fd9f2a7baf3" title="eccbc87e4b5ce2fe28308fd9f2a7baf3" href="/eccbc87e4b5ce2fe28308fd9f2a7baf3" coords="585,608,598,691,593,429,584,421" shape="poly">
22 <area target="" alt="a87ff679a2f3e71d9181a67b7542122c" title="a87ff679a2f3e71d9181a67b7542122c" href="/a87ff679a2f3e71d9181a67b7542122c" coords="658,658,644,437,658,652,655,437" shape="poly">
23 <area target="" alt="e4da3b7fbbce2345d7772b0674a318d5" title="e4da3b7fbbce2345d7772b0674a318d5" href="/e4da3b7fbbce2345d7772b0674a318d5" coords="692,637,690,455,695,628,695,467" shape="poly">
24 <area target="" alt="1679091c5a880faf6fb5e6087eb1b2dc" title="1679091c5a880faf6fb5e6087eb1b2dc" href="/1679091c5a880faf6fb5e6087eb1b2dc" coords="719,620,719,450,728,471,720,609" shape="poly">
25 <area target="" alt="8f14e45fcee167a5a36dedd4bea2543" title="8f14e45fcee167a5a36dedd4bea2543" href="/8f14e45fcee167a5a36dedd4bea2543" coords="857,612,833,610,936,456,852,455" shape="poly">
26 <area target="" alt="c9f0f895fb98ab9159f51fd0297e236d" title="c9f0f895fb98ab9159f51fd0297e236d" href="/c9f0f895fb98ab9159f51fd0297e236d" coords="1475,857,1473,354,1537,335,1541,901" shape="poly">
27 <area target="" alt="45c48cce2e2d7fbdea1afc51c7c6ad26" title="45c48cce2e2d7fbdea1afc51c7c6ad26" href="/45c48cce2e2d7fbdea1afc51c7c6ad26" coords="1324,766,1380,752,1380,401,1325,397" shape="poly">
28 <area target="" alt="d3d9446802a44259755d38e6d163e820" title="d3d9446802a44259755d38e6d163e820" href="/d3d9446802a44259755d38e6d163e820" coords="1202,695,1217,704,1222,423,1203,423" shape="poly">
29 <area target="" alt="6512bd43d9caa6e02c990b0a82652dca" title="6512bd43d9caa6e02c990b0a82652dca" href="/6512bd43d9caa6e02c990b0a82652dca" coords="1154,668,1146,661,1144,442,1157,442" shape="poly">
30 <area target="" alt="c20ad4d76fe97759aa27a0c99bfff6710" title="c20ad4d76fe97759aa27a0c99bfff6710" href="/c20ad4d76fe97759aa27a0c99bfff6710" coords="1185,628,1116,633,1113,447,1102,447" shape="poly">
31 <area target="" alt="c51ce410c124a10e0db5e4b97fc2af39" title="c51ce410c124a10e0db5e4b97fc2af39" href="/c51ce410c124a10e0db5e4b97fc2af39" coords="1073,609,1081,620,1082,459,1073,463" shape="poly">
32 </map>
33
34
35 </body>
36 </html>
```

Burada bizi yönlendirdiği tüm sub domainleri görüyoruz. Bu şifrelenmiş sub domainleri çözmek için hashcat aracını kullanıyoruz

Öncelikle hepsini bir yere kopyaladım

```
(root@berk)-[~/Documents/CTF/Corridor]
# cat veriler
c4ca4238a0b923820dcc509a6f75849b
c81e728d9d4c2f636f067f89cc14862c
eccbc87e4b5ce2fe28308fd9f2a7baf3
a87ff679a2f3e71d9181a67b7542122c
e4da3b7fbbce2345d7772b0674a318d5
1679091c5a880faf6fb5e6087eb1b2dc
8f14e45fcee167a5a36dedd4bea2543
c9f0f895fb98ab9159f51fd0297e236d
45c48cce2e2d7fbdea1afc51c7c6ad26
d3d9446802a44259755d38e6d163e820
6512bd43d9caa6e02c990b0a82652dca
c20ad4d76fe97759aa27a0c99bfff6710
c51ce410c124a10e0db5e4b97fc2af39
```

ve hashcat kullanarak bu verilerin hangi şifreleme türü ile şifrelendiğini buldum

```
(root@berk)-[~/Documents/CTF/Corridor]
# hashcat veriler
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-penryn-12th Gen Intel(R) Core(TM) i5-12500H, 2917/5899 MB (1024 MB allocatable), 8MCU

The following 11 hash-modes match the structure of your input hash:

# | Name | Category
=====|=====|=====
900 | MD4 | Raw Hash
0 | MD5 | Raw Hash
70 | md5(utf16le($pass)) | Raw Hash
2600 | md5(md5($pass)) | Raw Hash salted and/or iterated
3500 | md5(md5(md5($pass))) | Raw Hash salted and/or iterated
4400 | md5(sha1($pass)) | Raw Hash salted and/or iterated
20900 | md5(sha1($pass).md5($pass).sha1($pass)) | Raw Hash salted and/or iterated
4300 | md5(strtoupper(md5($pass))) | Raw Hash salted and/or iterated
1000 | NTLM | Operating System
9900 | Radmin2 | Operating System
8600 | Lotus Notes/Domino 5 | Enterprise Application Software (EAS)

Please specify the hash-mode with -m [hash-mode].

Started: Thu Sep 5 06:58:11 2024
Stopped: Thu Sep 5 06:58:14 2024
```

Bize md5 ile şifrelendiğini ve hashcat -m 0 komutunu kullanarak bu verileri çözebileceğimizi söylüyor

```
hashcat -m 0 veriler /usr/share/wordlists/rockyou.txt -o çözülmüşveriler.txt
```

```
(root@berk)-[~/Documents/CTF/Corridor]
# ls
çözülmüşveriler.txt veriler

(root@berk)-[~/Documents/CTF/Corridor]
# cat çözülmüşveriler.txt
c4ca4238a0b923820dcc509a6f75849b:1
c20ad4d76fe97759aa27a0c99bfff6710:12
6512bd43d9caa6e02c990b0a82652dca:11
c51ce410c124a10e0db5e4b97fc2af39:13
8f14e45fceeaa167a5a36dedd4bea2543:7
eccbc87e4b5ce2fe28308fd9f2a7baf3:3
d3d9446802a44259755d38e6d163e820:10
45c48cce2e2d7fbdea1afc51c7c6ad26:9
c81e728d9d4c2f636f067f89cc14862c:2
1679091c5a880faf6fb5e6087eb1b2dc:6
e4da3b7fbbce2345d7772b0674a318d5:5
c9f0f895fb98ab9159f51fd0297e236d:8
a87ff679a2f3e71d9181a67b7542122c:4
```

Görmüş olduğumuz gibi 1 den başlayarak 13 e kadar gidiyor. Şuan elimizde başka bir veri olmadığı için flagi bulmak için acaba öncesinde ve sonrasında da başka birşey varmı diye kontrol edebiliriz çünkü 1 den 13 e kadar belli bir düzende md5 hash algoritmasıyla devam etmiş şimdi gidip acaba 0 veya 14 varmı diye kontrol edelim. 0 ı denemek için 0 ı md5 algoritmasıyla hashliyorum bunu sizde md5 hash generator'den oluşturabilirsiniz.



# 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):

0

md5

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

MD5 Hash(es):

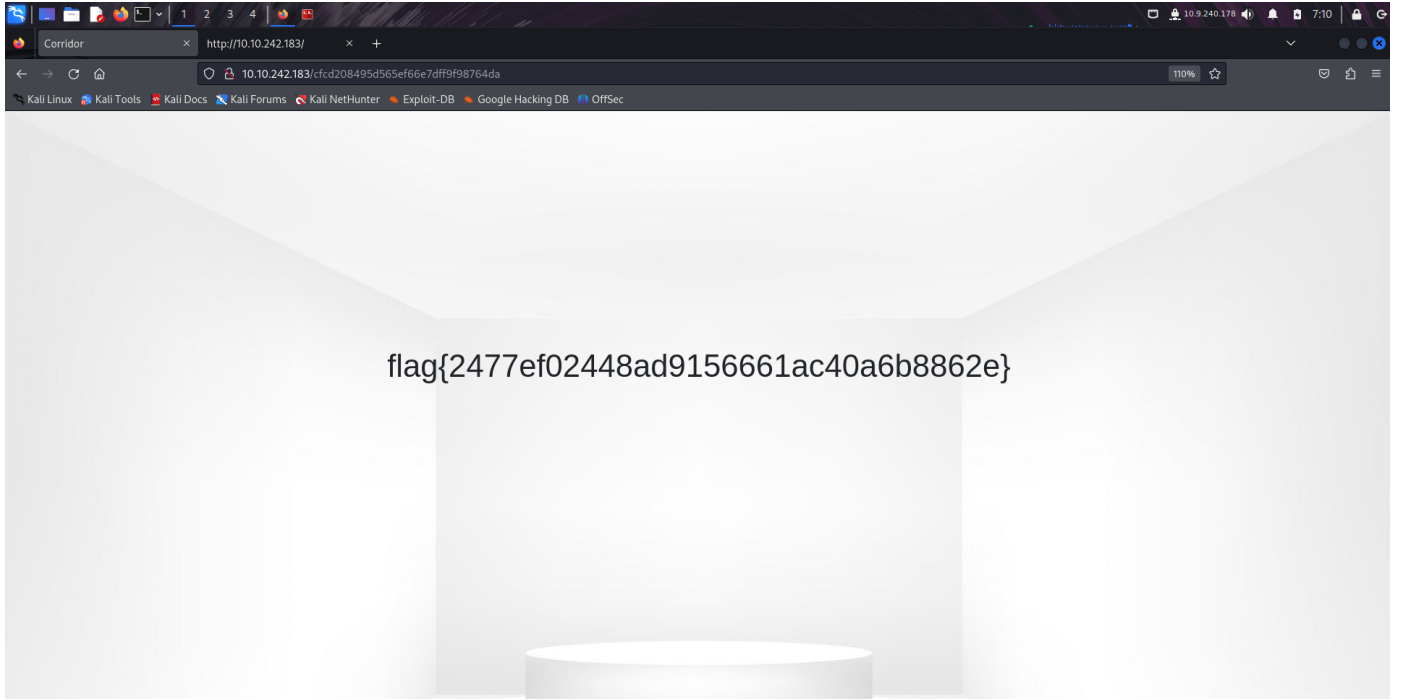
cfcd208495d565ef66e7dff9f98764da

**Privacy notice:** All content generated by this tool is done on your computer via client-side JavaScript whenever possible, or on the Miracle Salad server as a fallback if not. No submitted or generated data is recorded or stored by Miracle Salad. See the [website privacy statement](#) regarding general use of this website.

**Special note about line endings:** Mac/Unix and Windows use different codes to separate lines. **The tool on this page normalizes all line endings to a Line Feed (\n).** Other tools are available online if you need hashes specifically with Windows line endings (Carriage Return + Line Feed: \r\n).

**Reminder:** [MD5 is not a cryptographically secure hashing algorithm](#).

Vee evet bunu sub domain olarak denediğimizde flagimizi başarıyla almış oluyoruz



## Burada OWASP TOP 10 deki 2 güvenlik açığına değinmiş oluyoruz

- **A01:2021 - Broken Access Control (Bozuk Erişim Kontrolü):** Sistemde 0. bir kapının olması ve bu kapının güvenli şekilde gizlenmemesi, erişim kontrollerinin düzgün yapılandırılmadığını gösterir. Sadece URL'de bir md5 kodu değiştirerek yeni bir alan adına ulaşmak, güvenlik açısından zayıf bir uygulamadır.
- **A05:2021 - Security Misconfiguration (Güvenlik Yanlış Yapılandırması):** Gizli bir sub domainin basit bir md5 kodlamasıyla erişilebilir olması, yanlış yapılandırma veya yeterince güvenli olmama ile ilgili bir soruna işaret eder.

Umarım yararlı olmuştur başka bir CTF'de görüşmek üzere

**Ayberk İlbaş**

[Linkedin](#)

[Github](#)

[Instagram](#)