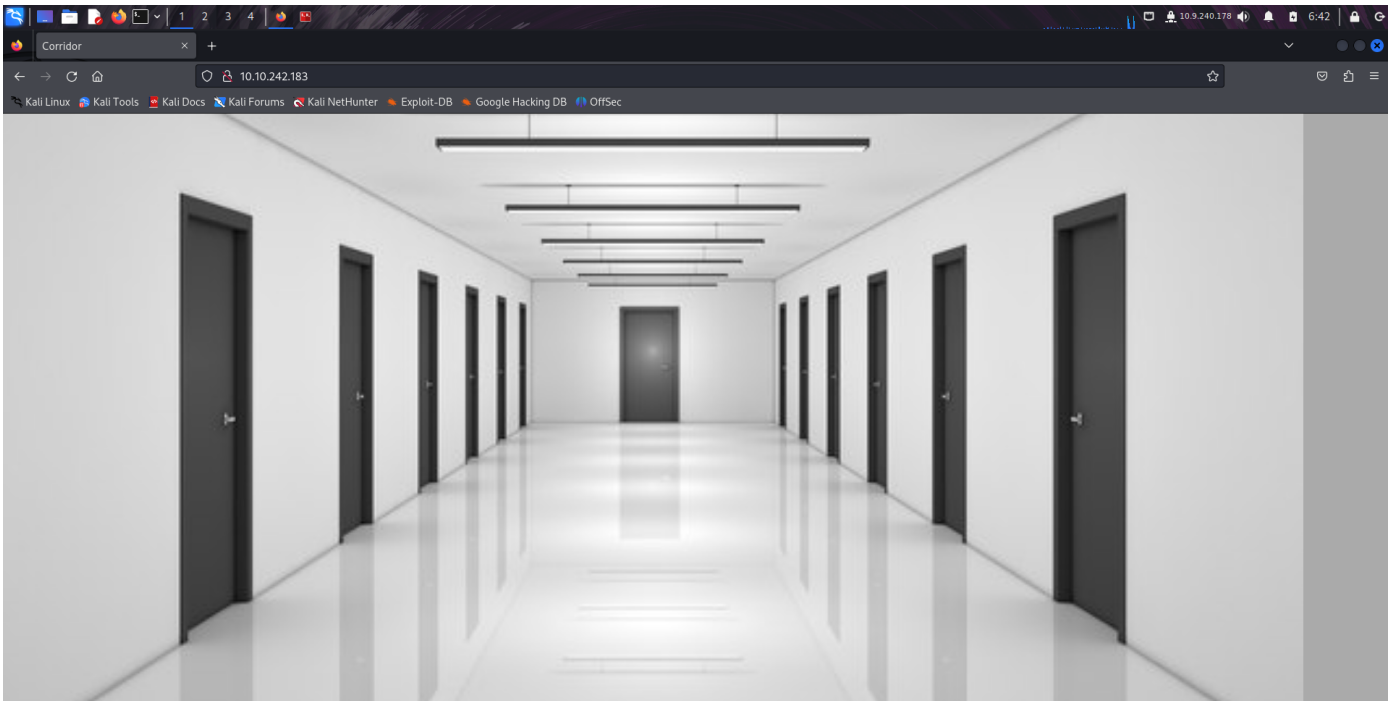
Corridor CTF Walkthrough

Merhaba, bugün sizlerle TryHackMe platformunda yer alan 'Corridor' adlı CTF'i beraber çözeceğiz.

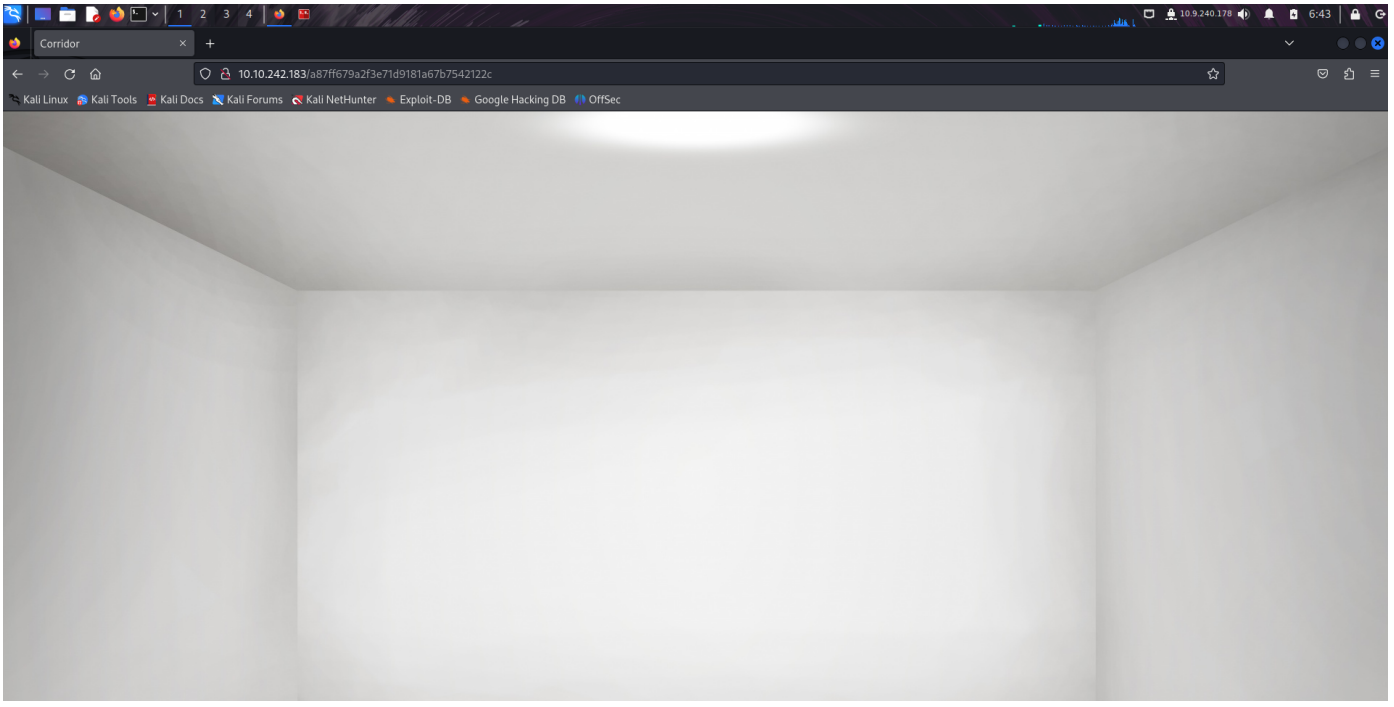
Taramayla başlayalım

Öncelikle tüm portları hızlıca taramak için rustscan aracını kullanalım `rustscan -a <ip adresi>`

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

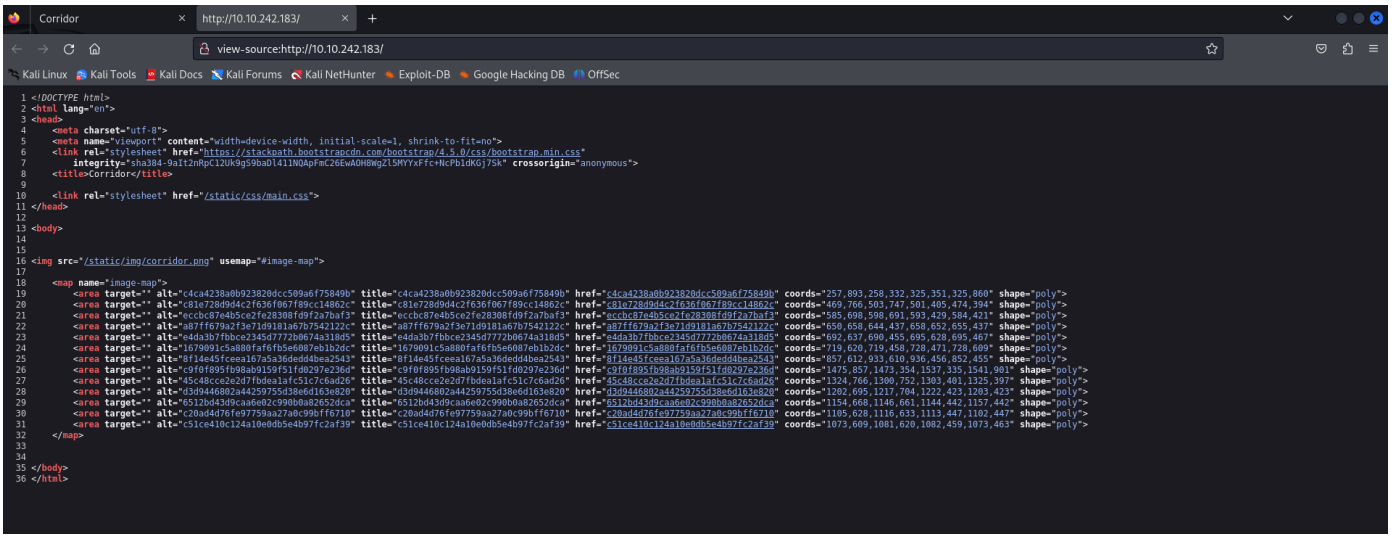


Web sitesine girdiğimizde bizi böyle bir sayfa karşılıyor.



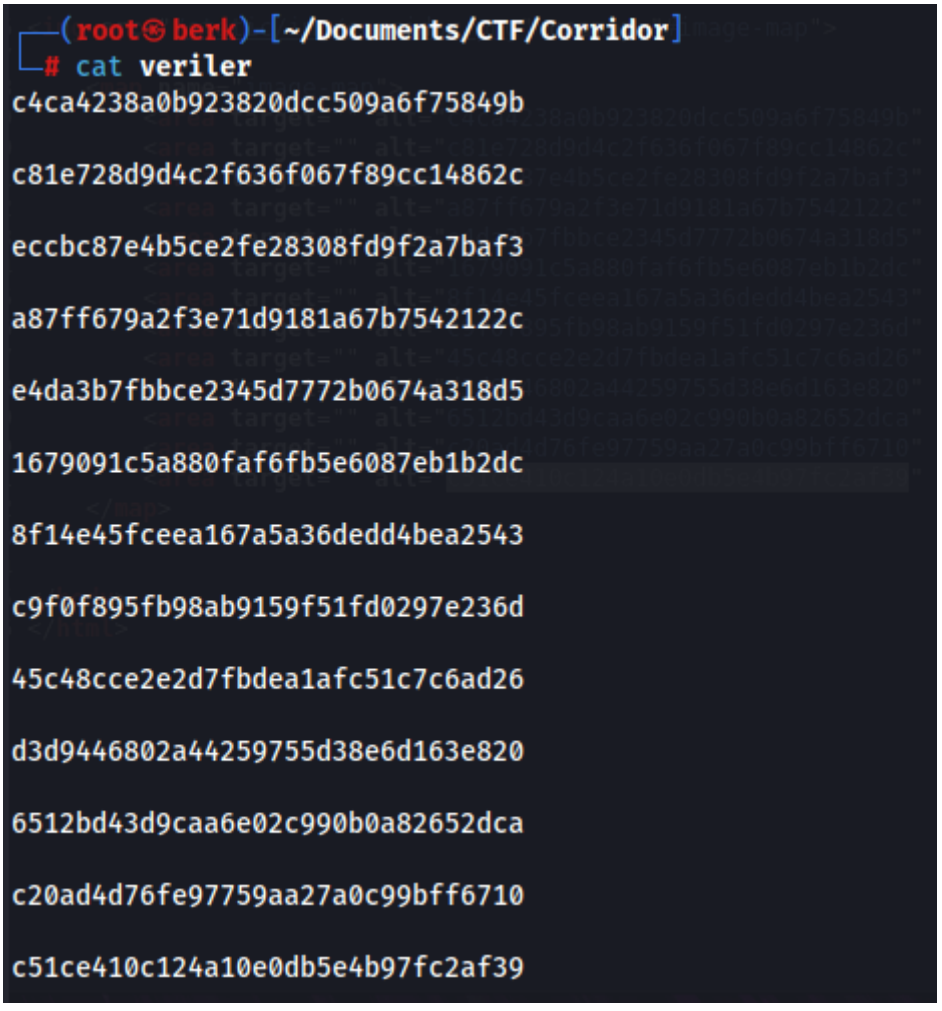
Kapılara tıkladığımızda ise bizi böyle boş odalara yönlendiriyor. Urlde bizi yönlendirdiği sub domain şifrelenmiş olarak gözüküyor

Sayfanın kaynak kodlarına baktığımızda ise



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

Öncelikle hepsini bir yere kopyaladım



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
```

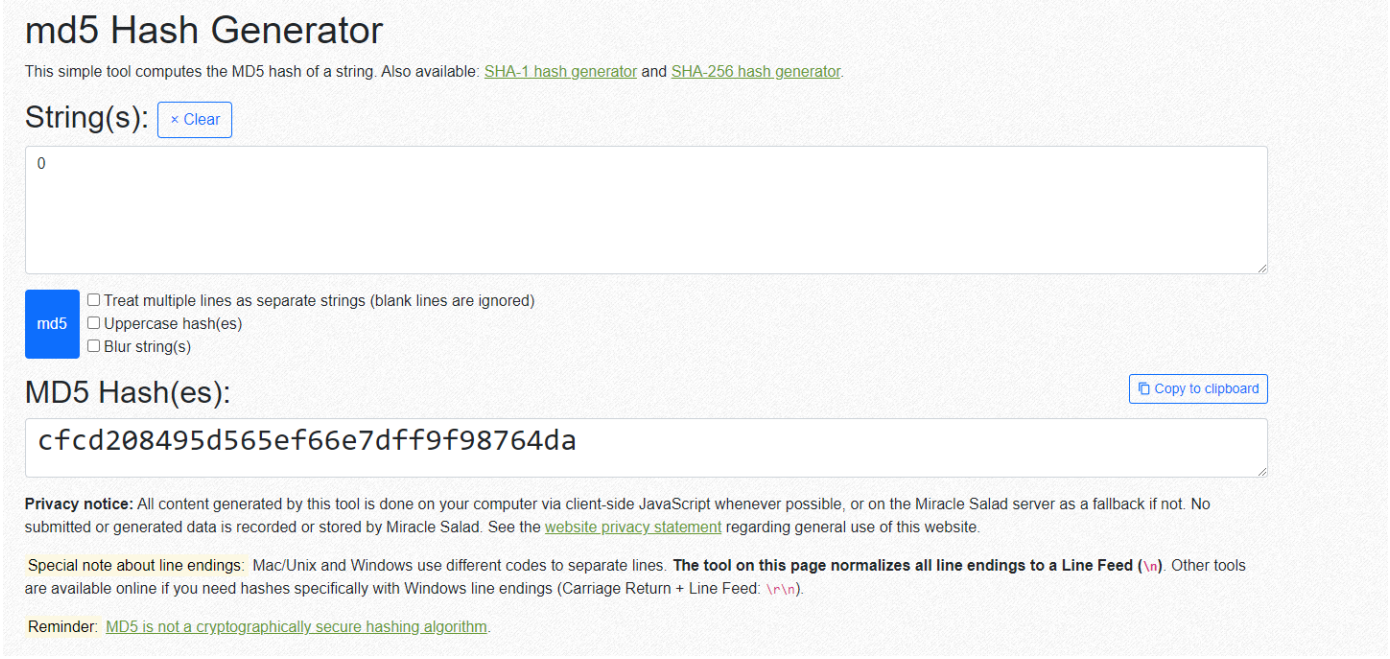
Bize md5 ile şifrelendiğini ve hashcat -m 0 komutunu kullanarak bu verileri çözebileceğimizi söylüyor

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

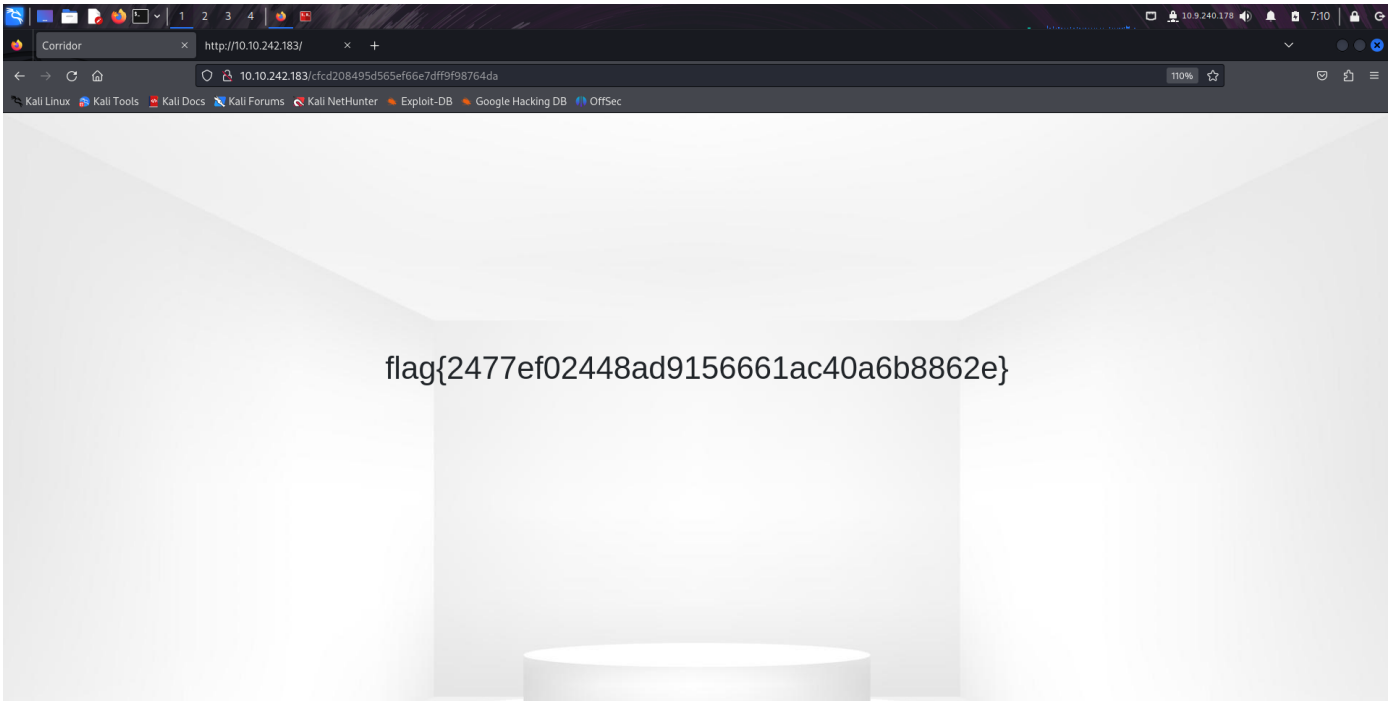
```
┌──(root㉿berk)-[~/Documents/CTF/Corridor]
└─# ls
çözülmüsveriler.txt  veriler

┌──(root㉿berk)-[~/Documents/CTF/Corridor]
└─# cat çözülmüsveriler.txt
c4ca4238a0b923820dcc509a6f75849b:1
c20ad4d76fe97759aa27a0c99bff6710:12
6512bd43d9caa6e02c990b0a82652dca:11
c51ce410c124a10e0db5e4b97fc2af39:13
8f14e45fceea167a5a36dedd4bea2543:7
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.



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

İnstagram