BRUTE FORCE

Aysu Yiğit 211106206007
Latife Yılmaz 200106206002
Emre Can Çavuş 212106206003

BRUTE FORCE NEDİR?

Brute force attack bir kaba kuvvet saldırısıdır.

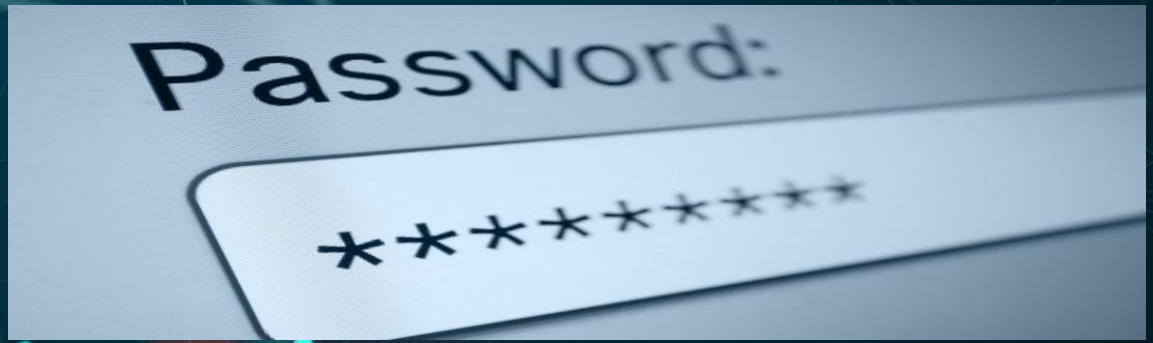
Brute force attack, bir bilgisayar sistemine veya şifrelenmiş verilere erişim sağlamak amacıyla, tüm olası kombinasyonları deneyerek şifreyi kırmaya çalışan bir siber saldırı türüdür.

BRUTE FORCE SALDIRILARINA KARŞI ALINABİLECEK ÖNLEMLER

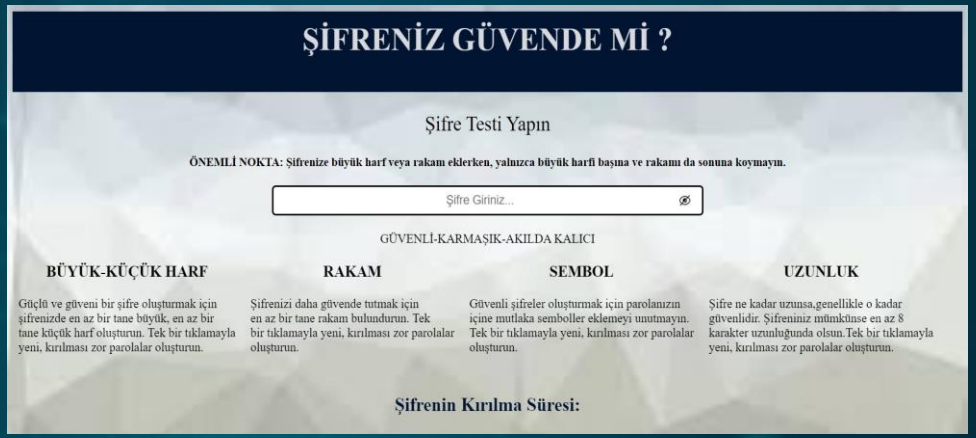
1. Güçlü Şifreler Kullanımı
2. Çift Faktörlü Kimlik Doğrulama (2FA)
3. Oturum Açma Denemelerini Sınırlayın
4. IP Adresi Tabanlı Sınırlamalar
5. Güvenlik Duvarları ve IPS Kullanımı
6. Güvenlik Bilinci Eğitimi
7. Güncel Yazılım ve Sistemler
8. Log Takibi ve İzleme

Projemizin Amacı ?

Projemizde, güçlü şifrelerin güvenliği hakkında farkındalık yaratmayı ve kullanıcılara şifre gücünü ölçen bir araç sunmayı amaçlıyoruz. Kullanıcılar, belirli bir şifrenin ne kadar sürede kırılabileceğini tahmin etmek ve daha güçlü şifreler oluşturmak konusunda bilinçlenmek için bu aracı kullanabilirler. Bu, siber güvenlik bilincini artırabilir ve güvenli şifre uygulamalarını teşvik edebilir.



Projemiz Nedir ?



Projemiz brute force attackslarından korunmak için güçlü şifre ürütmek üzerine. Bu konudan yola çıkarak şifrenin güvenirliğini ölçen ve her girdide şifrenin kırılma süresini yaklaşık olarak hesaplayan bir web sitesi kurmaktır.

Yöntem

"zxcvbn" Kütüphanesi

zxcvbn, şifre güvenliğini değerlendirmek için kullanılan bir JavaScript kütüphanesidir. Bu kütüphane, kullanıcıların oluşturdukları şifrelerin gücünü ve dayanıklılığını analiz eder. Genellikle şifre politikalarını uygulamak, kullanıcılara daha güvenli şifreler oluşturmaları konusunda rehberlik etmek ve şifre zayıflıklarını tespit etmek için kullanılır.

Elde edilen sonuç nesnesi, şifrenin güvenlik puanı, tahmini kırılma süresi ve öneriler gibi bilgileri içerir. Bu bilgiler, kullanıcılara daha güvenli şifreler oluşturmaları konusunda rehberlik etmek için kullanılabilir.