**Cangibrina Nedir?**

Cangibrina, özellikle web uygulamalarına yönelik yapılan sızma testlerinde kullanılan bir güvenlik aracıdır. Temel olarak **brute-force (kaba kuvvet)** saldırıları ve **SQL injection** (SQL enjeksiyonu) denemeleri yapmak için tasarlanmıştır. Kullanıcıların zayıf şifrelerini veya sistemlerdeki güvenlik açıklarını tespit etmeye yardımcı olur.

**Cangibrina’nın Özellikleri**

* **Brute-force saldırısı** yapabilir: Belirlenen kullanıcı adı ve parola listeleriyle deneme yapar.
* **SQL Injection denemeleri** yapabilir: Web uygulamalarındaki veri tabanı sorgularını manipüle ederek açıklara ulaşmaya çalışır.
* Otomatik tarama yapabilir, hedef web sitesine veya uygulamaya karşı hızlı testler gerçekleştirir.
* Komut satırı tabanlı veya GUI (grafik arayüzlü) olabilir (kullandığın versiyona bağlı).
* Açık kaynak kodlu ve ücretsiz olabilir (versiyonuna göre değişir).

**Kullanım Alanları:**

* **Penetrasyon testleri:** Sistem yöneticileri veya güvenlik uzmanları tarafından zayıf noktaları keşfetmek için kullanılır.
* **Siber güvenlik eğitimleri:** Öğrenciler ve uzman adayları için pratik araçtır.
* **Zafiyet değerlendirmesi:** Web uygulamalarının güvenlik durumunun analizinde tercih edilir.
* **Saldırı simülasyonları:** Gerçek saldırı senaryolarını canlandırarak savunma yöntemleri geliştirilir.

**Kurulum Aşamaları:**

Cangibrina’nın kurulumu kullanılan işletim sistemine göre değişir ama genelde şu adımlar takip edilir:

1. **Araç dosyasını indirme:** GitHub veya resmi kaynaklardan indirilir.
2. **Bağımlılıkların yüklenmesi:** Python veya diğer dillerde yazıldıysa, gerekli kütüphaneler (örneğin requests, beautifulsoup4 gibi) yüklenir.
3. **Araç dosyasının konfigürasyonu:** Hedef site veya IP adresi, kullanıcı listesi, parola listesi gibi parametreler ayarlanır.
4. **Çalıştırma:** Komut satırı üzerinden veya GUI’den tarama başlatılır.
5. **Sonuçların değerlendirilmesi:** Araç tarafından raporlanan açıklar incelenir.

**Dikkat Edilmesi Gereken Noktalar:**

* **Yasal izin olmadan kullanmayın!** Cangibrina gibi araçlar izinsiz kullanılırsa suç teşkil eder.
* Hedef sistemin performansını olumsuz etkileyebilir; yoğun taramalar sistemde kesintilere neden olabilir.
* Brute-force denemeleri çok sayıda başarısız girişe sebep olacağı için IP engellemelerine yol açabilir.
* SQL Injection denemeleri sistemde veri kaybına veya güvenlik açığının büyümesine neden olabilir; dikkatli olunmalıdır.
* Araç güncellemeleri ve sürüm uyumluluğu takip edilmelidir.
* Güvenlik testleri için sadece kendi sistemleriniz veya izinli sistemlerde kullanılmalıdır.