**TIDoS-Framework**

**TIDoS-Framework Nedir?**

TIDoS-Framework, web uygulamalarının güvenlik açıklarını keşfetmek için tasarlanmış kapsamlı bir saldırı yüzeyi analiz aracıdır. Açık kaynaklıdır ve hem bilgi toplama hem de zafiyet tespitinde kullanılır.

**Özellikleri:**

•400’den fazla modül: Bilgi toplama, zafiyet analizi, sömürü (exploit) testleri gibi geniş kapsamlı araçlar içerir.

•Otomatik tarama: Hedef üzerinde detaylı güvenlik analizi yapabilir.

•Manuel test imkânı: Gelişmiş kullanıcılar için özelleştirilmiş modüller sunar.

•Raporlama: Sonuçları detaylı şekilde listeler.

•Platform bağımsız: Linux, macOS ve Windows üzerinde çalışabilir.

**Kullanım Alanları:**

✓Penetrasyon testlerinde hedef web uygulamasının zafiyetlerini belirleme.

✓Alt alan adı keşfi, port taraması, servis analizi gibi bilgi toplama süreçleri.

✓SQL Injection, XSS gibi yaygın güvenlik açıklarını tespit etme.

✓Güvenlik araştırmalarında geniş kapsamlı saldırı yüzeyi analizi.

**Kurulum Aşamaları:**

**1. Python 3 kurulu olduğundan emin olun.**

**2**. Depoyu klonlayın: 

**3**. Dizine girin:



**4**. Gerekli bağımlılıkları yükleyin:



**5**. Framework’ü çalıştırın: 

**Dikkat Edilmesi Gerekenler:**

✓Araç birçok modül içerdiğinden tarama süresi uzun olabilir; yalnızca gerekli modülleri seçmek zaman kazandırır.

✓Yasal izin alınmamış sistemlerde kullanılması suç teşkil eder; yalnızca yetkili hedeflerde çalıştırılmalıdır.

✓Büyük ölçekli taramalarda ağ trafiği yoğunlaşabilir, hız ayarlarını kontrollü yapmak faydalıdır.

✓Güncel versiyonu kullanmak, hataların ve yanlış pozitiflerin azalmasına yardımcı olur.