**Burp Suite**

**Burp Suite Nedir?**

Burp Suite, web uygulama güvenliği testleri için kullanılan gelişmiş bir sızma testi (penetration testing) aracıdır. Özellikle web sitelerindeki zafiyetleri (açıkları) tespit etmek, analiz etmek ve istismar etmek için kullanılır.

-Burp Suite, bir web sitesini içeriden dışarıya kadar didik didik eden ve açık arayan bir “siber güvenlik büyüteci” gibidir.

**Burp Suite'in Özellikleri**

* **Proxy:** Tarayıcı ile hedef web sitesi arasındaki trafiği yakalar ve değiştirmene izin verir.
* **Scanner (sadece Pro sürüm):** Otomatik zafiyet taraması yapar (örnek: XSS, SQLi).
* **Intruder:** Belirli parametrelere göre saldırı (brute-force, payload) gerçekleştirir.
* **Repeater:** Aynı isteği tekrar tekrar düzenleyip göndererek test yapma imkânı.
* **Decoder & Comparer:** Verileri şifreleme/çözme veya iki veriyi karşılaştırma modülü.
* Hem manuel hem otomatik test imkânı sağlar.

**Kullanım Alanları**

* **Etik hackerlar (pentester):** Web uygulama açıklarını test eder.
* **Siber güvenlik analistleri:** Uygulama güvenliğini değerlendirir.
* **Geliştiriciler:** Web uygulamalarında hangi açıklara karşı önlem alacaklarını test eder.
* **Eğitim:** Zafiyetli uygulamalarda güvenlik test pratiği yapılmasını sağlar.

**Kurulum Aşamaları:**

**Windows/Linux için Kurulum:**

1. **Resmi web sitesine gir:**  
    https://portswigger.net/burp
2. Ücretsiz sürümü indirmek için:
   * “**Burp Suite Community Edition**” seçeneğine tıkla.
   * İşletim sistemine uygun versiyonu indir (.exe veya .jar).
3. **Windows için:**
   * .exe dosyasını çalıştır ve “Next” diyerek kurulumu tamamla.
4. **Linux için:**
   * .sh veya .jar uzantılı dosya indirilebilir.

-Terminal üzerinden şu komutla çalıştırabilirsin:



1. Tarayıcı ayarlarında proxy olarak 127.0.0.1:8080 ayarlanmalı.
2. Gerekirse Burp’ın sertifikası yüklenerek HTTPS trafiği de izlenebilir.

**Dikkat Edilmesi Gerekenler:**

* **İzinsiz test yapmak yasa dışıdır.** Sadece kendi sisteminde veya izin aldığın sistemlerde test yapmalısın.
* Ücretsiz sürümde otomatik tarayıcı (scanner) özelliği sınırlıdır.
* HTTPS trafiği izlemek için güvenlik sertifikası yüklenmelidir; bu bazı sistemlerde risk oluşturabilir.
* Proxy yapılandırmasını yaparken dikkatli olunmalıdır, aksi takdirde bağlantı sorunları oluşabilir.
* Çok güçlü bir araç olduğu için yanlış yapılandırmalar sistemlere zarar verebilir.