**🧠 1. Fiddler Nedir?**

**Fiddler**, HTTP/HTTPS trafiğini yakalamak, incelemek ve değiştirmek için kullanılan bir **proxy tabanlı trafik analiz aracıdır**.

* Windows, macOS ve Linux üzerinde çalışabilir
* Web tarayıcılar, mobil cihazlar veya masaüstü uygulamalarından gelen trafiği analiz edebilir
* İstek ve yanıt içeriklerini düzenleyerek test yapılmasına izin verir

📌 Özellikle **web uygulama güvenlik testleri**, **API debugging** ve **performans analizi** için yaygın kullanılır.

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 📡 Trafik yakalama | HTTP ve HTTPS istek/yanıtlarını görüntüleme |
| 🛠️ İstek manipülasyonu | Header, cookie ve body değiştirme |
| 🔍 API testi | REST ve SOAP API trafiğini analiz etme |
| ⚡ Performans ölçümü | İstek yanıt sürelerini ölçme |
| 🔑 SSL/TLS analizleri | Sertifika hatalarını ve yapılandırma sorunlarını görme |

**⚙️ 3. Kurulum (Windows / Linux / macOS)**

**✅ 1. İndirme:**

* https://www.telerik.com/fiddler adresinden işletim sisteminize uygun sürümü indirin.

**✅ 2. Kurulum ve başlatma:**

* Kurulum tamamlandıktan sonra Fiddler başlatılır ve **default olarak 127.0.0.1:8888** üzerinden proxy olarak dinlemeye başlar.

**✅ 3. HTTPS trafiği için:**

* **Tools → Options → HTTPS → Decrypt HTTPS traffic** seçeneğini aktif edin.
* SSL sertifikasını yükleyerek şifreli trafiği çözümleyebilirsiniz.

**🚀 4. Kullanım Adımları**

**✅ 1. Trafik yakalama başlatma/durdurma:**

* **F12** ile capture modunu açıp kapatabilirsiniz.

**✅ 2. Belirli bir isteği inceleme:**

* Sol panelden isteği seçerek **Inspectors** sekmesinden ayrıntılara bakabilirsiniz.

**✅ 3. İstek değiştirme (Composer):**

* **Composer** sekmesinden yeni HTTP isteği oluşturabilir veya mevcut isteği düzenleyip yeniden gönderebilirsiniz.

**✅ 4. Filtreleme:**

* **Filters** sekmesi ile sadece belirli domain veya IP’lerden gelen trafiği görebilirsiniz.

**📋 5. Örnek Kullanım Senaryoları**

| **Senaryo** | **Açıklama** |
| --- | --- |
| 🧠 Web güvenlik testi | XSS, SQLi gibi zafiyetlerin manuel testi |
| 🔍 API debugging | API isteği/yanıtı analiz etme |
| 🛡️ Blue Team izleme | İstenmeyen trafik tespiti |
| 🧪 Mobil uygulama testi | Mobil cihaz trafiğini analiz etme |
| ⚡ Performans ölçümü | Yavaş yüklenen endpoint’leri belirleme |

**📡 6. Örnek Fiddler Trafik Analizi Çıktısı**

metin, ekran görüntüsü, multimedya, küçük alet içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🎯 7. Öğrenim Kazanımları**

* HTTP/HTTPS trafiğini yakalama ve analiz etme
* İstek/yanıt manipülasyonu ile güvenlik testi yapma
* API debugging süreçlerine hâkim olma
* SSL/TLS yapılandırma hatalarını tespit etme
* Proxy tabanlı trafik analiz araçlarının kullanımına aşinalık kazanma