# Burp Suite GraphQL Raider - Eğitim Materyali

## 🔍 Burp Suite GraphQL Raider Nedir?

GraphQL Raider, Burp Suite üzerine kurulan bir eklentidir (extension) ve GraphQL API’lerini test etmek için özel olarak geliştirilmiştir.  
  
- Burp Suite’in Extender bölümünden yüklenir  
- GraphQL endpoint'lerini keşfeder  
- Otomatik introspection sorguları göndererek şema yapısını çözer  
- Güvenlik açıklarını (yetki atlama, XSS, SQLi vb.) test etmeye olanak tanır

## ⚙️ Temel Özellikler

- 🧠 Introspection desteği: GraphQL şemasını otomatik çıkarır  
- 🔍 Otomatik sorgu üretimi: Girdi noktalarını analiz eder  
- 🧪 Fuzzing yeteneği: Parametreler üzerinde otomatik zafiyet testi  
- 🧾 Query, mutation ayrımı: Hedef API’nin yapısına göre ayrım yapar

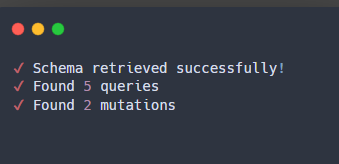
## 💻 Kurulum (Burp Suite Üzerinden)

1. Burp Suite’i başlatın  
2. Üst menüden Extender > BApp Store'a gidin  
3. GraphQL Raider eklentisini bulun ve yükleyin  
4. Yükleme sonrası menüde “GraphQL Raider” sekmesi belirecektir  
  
📌 Gereklilik: Java destekli Burp Suite (Community veya Pro)

## 🧪 Kullanım Örnekleri

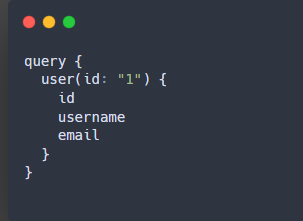
### ✅ Örnek 1: Introspection (Şema Çözümleme)

1. Burp ile hedef siteye tarayıcı üzerinden istek gönderin  
2. GraphQL Raider sekmesine geçin  
3. “Introspect” butonuna tıklayın  
4. Sonuç olarak şemada yer alan tüm query ve mutation yapıları listelenir



### ✅ Örnek 2: Manual Query Testi

Manuel bir query yazın ve gönderin:

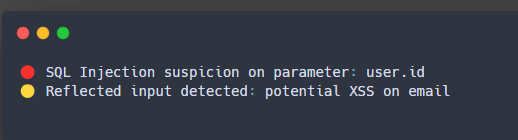


Örnek çıktı:



### ✅ Örnek 3: Fuzzing Testi

1. “Fuzzer” sekmesine geçin  
2. Otomatik olarak input parametrelerine payload'lar gönderilir  
3. Zafiyet bulgusu varsa işaretlenir



## ⚠️ Öğrenciler İçin Önemli Notlar (GraphQL Raider)

🎯 1. GraphQL API’ler Genelde Hassastır:  
Şema verileri sistem hakkında çok fazla bilgi verir. Bunları gerçek sistemlerde kullanmak yasal risk oluşturur.  
  
🧠 2. Introspection Her Zaman Açık Olmayabilir:  
Bazı sistemlerde introspection kapalıdır. Bu durumda manuel sorgu denemeleri yapılmalıdır.  
  
🧪 3. Test Ortamlarında Kullan:  
Gerçek verilerle oynamadan önce mutlaka test sunucusunda çalışma yapılmalıdır.