## **Autorize Nedir?**

**Autorize**, web uygulamalarındaki **yetkilendirme (authorization)** kontrollerinin doğru şekilde uygulanıp uygulanmadığını test etmeye yarayan bir **Burp Suite eklentisidir**.  
Amaç, kullanıcı rollerinin sınırlarını test ederek, bir kullanıcının **izin verilmemiş işlemleri yapıp yapamayacağını** belirlemektir.

Örneğin, bir normal kullanıcı admin paneline erişmeye çalıştığında sistem buna izin veriyor mu? Ya da başka bir kullanıcının hesabına ait verileri görebiliyor mu?

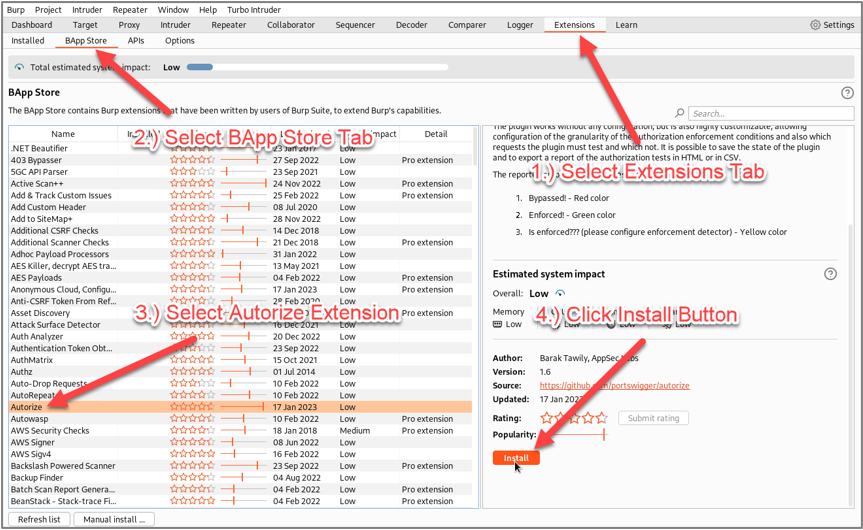
Autorize, bu tür durumları **otomatik test etmenizi sağlayan pratik bir araç**tır.

## **Neden Kullanılır?**

Web uygulamalarında, kimlik doğrulama (authentication) genellikle doğru yapılandırılırken, **yetkilendirme (authorization)** ihlalleri sıkça gözden kaçar. Bu tür açıklar genellikle şu zafiyetlere neden olur:

* **IDOR (Insecure Direct Object Reference)**
* **Vertical privilege escalation** (örneğin: kullanıcı → admin geçişi)
* **Horizontal privilege escalation** (örneğin: kullanıcıA → kullanıcıB verileri erişimi)

**Autorize**, farklı yetkilere sahip kullanıcı oturumlarıyla aynı isteği tekrar göndererek sistemin nasıl davrandığını gözlemler. Hatalı bir davranış varsa, bunu tespit eder.



## **Kullanım Örneği**

1. **Burp Suite'i aç** ve Autorize eklentisini yükle (BApp Store üzerinden).
2. Taramak istediğin hedefte, **önce normal kullanıcı**, ardından **yetkili kullanıcı** ya da **admin** ile oturum aç.
3. Autorize sekmesine gel ve aşağıdaki ayarları yap:
   * **Original request**: Taratılacak istekleri Burp Proxy’den gönder.
   * **Unauthorized token**: Yetkisiz kullanıcının Cookie, Authorization veya Header bilgisi.
   * **Authorized token**: Yetkili kullanıcının bilgisi.
   * Autorize bu iki kullanıcı arasında testler yapar ve yetkilendirme hatalarını tespit eder.
4. İstek gönderildikçe Autorize, hem yetkili hem yetkisiz kullanıcı adına aynı isteği tekrarlar ve gelen yanıtları karşılaştırır.

## Elde Edilen Sonuçlar

Tarama sonucunda aşağıdakiler tespit edilebilir:

* Normal kullanıcı, **admin işlemi** gerçekleştirebiliyor mu?
* Bir kullanıcı, başka kullanıcıya ait **verileri okuyabiliyor veya silebiliyor mu?**
* Sistemin belirli isteklerde **rol kontrolü yapmadığı** durumlar

Sonuçlar Autorize sekmesinde renkli olarak gösterilir:

* **Authorized**: Erişim doğru şekilde verilmiş.
* **Unauthorized access detected**: Yetkisiz kullanıcı, yetkili işlemi yapabiliyor.
* **Suspicious**: Davranış farklı ama kesin değil, manuel analiz önerilir.

## Öne Çıkan Özellikleri

* Farklı kullanıcı oturumları arasında **otomatik istek kıyaslaması**
* Token veya Cookie temelli test desteği
* Yanıtların otomatik olarak fark analizine tabi tutulması
* JSON gövdeleri dahil karmaşık istekleri destekleme
* Repeater veya Proxy'den kolay istek aktarımı