### Burp Suite Nedir?

İnternette en yaygın kullanılan ve özellikle siber güvenlik uzmanları tarafından sıklıkla tercih edilen **Burp Suite**, bir **web güvenlik test platformudur**. Burp Suite'in nasıl kurulduğuna geçmeden önce, temel bileşenlerinden biri olan **proxy sunucusu (veya HTTP proxy)** kavramını anlamamız gerekir.

### Proxy Sunucusu Nedir?

**Proxy sunucusu** (veya ara sunucu), istemci ile hedef sunucu arasında yer alan bir aracıdır. Tarayıcınızdan bir web sitesine erişmek istediğinizde, bu istekler doğrudan hedefe değil, önce proxy sunucusuna gider. Proxy bu isteği analiz eder, gerekirse değiştirir veya kaydeder ve ardından hedef sunucuya iletir.

* Proxy sunucusu LAN (yerel ağ) veya WAN (internet) üzerinde konumlanabilir.
* Proxy sunucusu, gelen istekleri **engelleme, izin verme, yönlendirme, değiştirme veya loglama (kayıt altına alma)** gibi işlemleri gerçekleştirebilir.
* Bir proxy kullanıldığında, dış dünyaya görünen IP adresi genellikle sizin değil, proxy sunucusunun IP adresidir.
* Proxy sadece web için değil; **ağ güvenliği, içerik filtreleme, önbellekleme, e-posta trafiği** gibi birçok alanda kullanılır.

### Burp Suite'e Genel Bakış

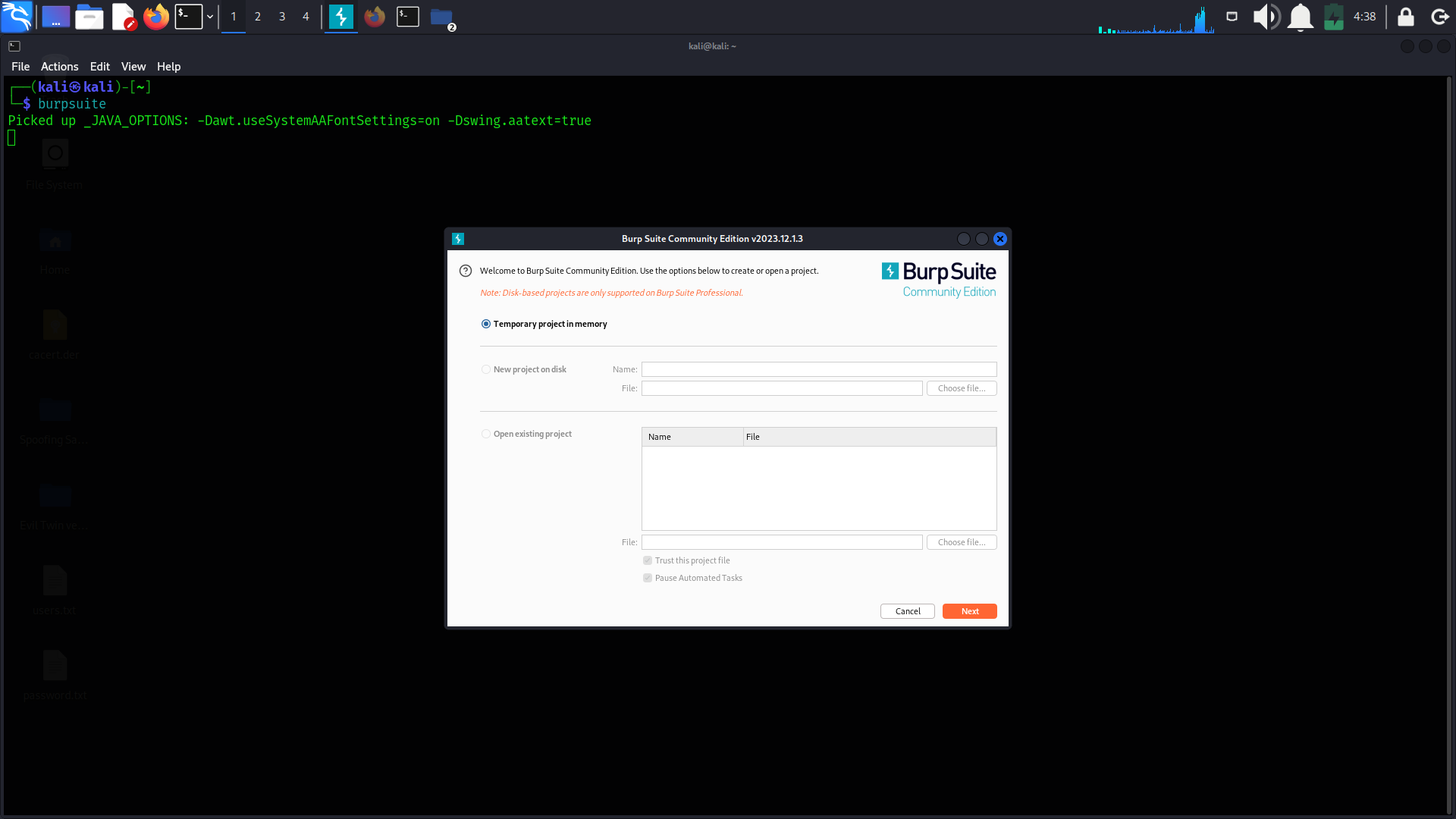
**Burp Suite**, web uygulama güvenliği testleri için geliştirilmiş **entegre bir araç setidir**. Ana işlevleri şunlardır:

* Web trafiğini **yakalama (interception)** ve **analiz etme**
* Web uygulamalarında **güvenlik açıklarını tespit etme**
* **Otomatik ve manuel saldırı tekniklerini simüle etme**
* Özellikle OWASP Top 10 açıklarını tespit etmede etkilidir

Burp Suite’in bileşenleri arasında şunlar yer alır:

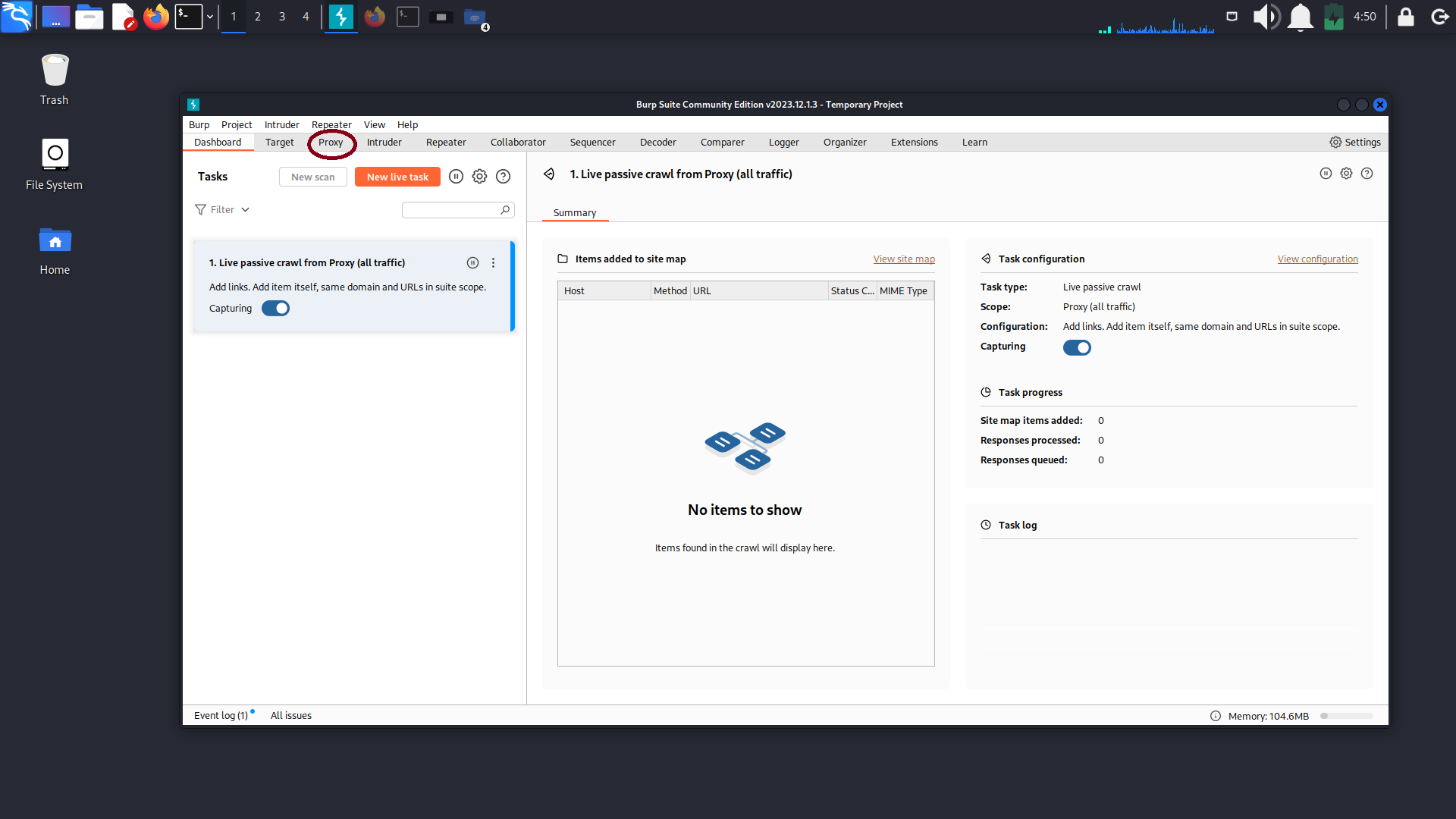
* **Proxy**: Tarayıcı trafiğini yakalayıp düzenleme
* **Intruder**: Brute-force ve payload testleri
* **Repeater**: Manuel olarak istekleri tekrar gönderme
* **Scanner** (sadece Professional sürümde): Otomatik zafiyet taraması
* **Decoder**, **Comparer**, **Extender** vb.

Kali Linux, Burp Suite'in Community Edition sürümünü ön yüklü olarak içerir. Terminalden şu komutla çalıştırabilirsiniz:



2. Arayüz açıldığında next ve start diyerek Burp Suite'i açıyoruz.

3. Daha sonra Proxy’ye tıklıyoruz.



### Intercept Nedir? (Burp Suite Proxy Özelliği)

Burp Suite’in en temel bileşenlerinden biri olan **Intercept**, web tarayıcısı ile hedef sunucu arasında geçen HTTP/S trafiğini **yakalamamıza, görüntülememize ve müdahale etmemize** olanak tanır.

#### Intercept Kapalı (Intercept is off):

* **Gelen ve giden istekler doğrudan sunucuya iletilir.**
* Burp Suite, bu trafiği yalnızca **izler ve kaydeder**, **müdahale etmez**.
* Bu mod, sadece trafik analizinde kullanılır; değişiklik yapılamaz.

#### Intercept Açık (Intercept is on):

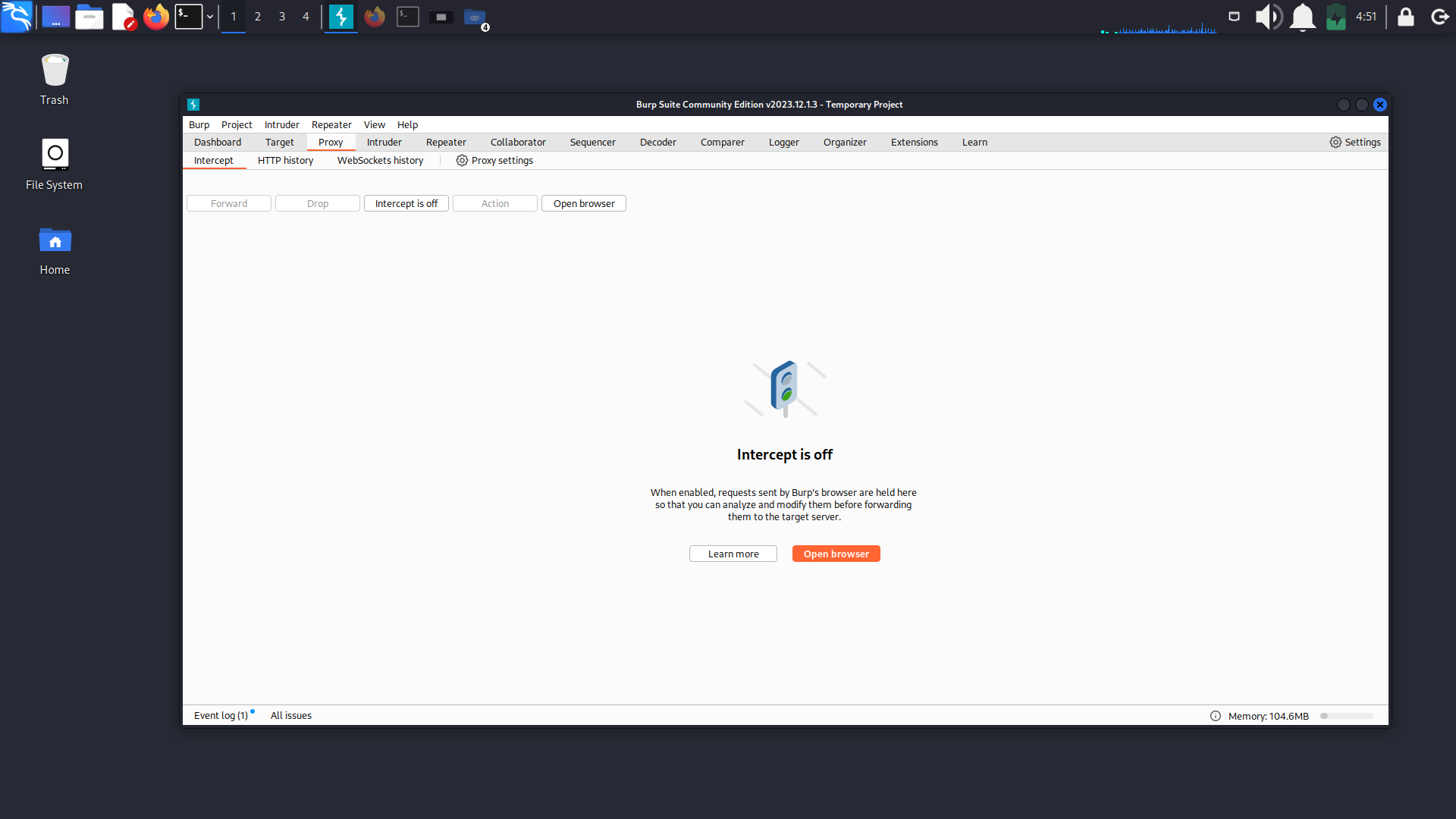
* **Tarayıcıdan sunucuya gönderilen tüm HTTP/S istekleri durdurulur** ve Burp Suite arayüzünde yakalanır.
* Burp, isteği tutar ve kullanıcıdan bir işlem bekler. Bu mod sayesinde aşağıdaki işlemler yapılabilir:

##### • Forward (İlet):

İstek, olduğu gibi **hedef sunucuya gönderilir**. Ardından, sunucunun yanıtı yakalanır ve Proxy → HTTP history sekmesinde görüntülenebilir.

##### • Drop (Bırak):

İstek **sunucuya iletilmeden iptal edilir**. Bu işlemle hedef uygulamanın ilgili isteği hiçbir zaman alması engellenmiş olur.



### Repeater Nedir?

**Repeater**, yakalanan bir isteği **manüel olarak tekrar tekrar göndermeye** ve **her denemede içeriğini değiştirmeye** yarar. Bu özellik sayesinde, örneğin aynı endpoint’e farklı payload’lar deneyerek **XSS, SQLi gibi zafiyetleri adım adım test edebilirsiniz**. Yakalanan bir istek sağ tıklanarak "Send to Repeater" seçilir ardından Repeater sekmesinde düzenlenip gönderilir.

### 

### Intruder Nedir?

**Intruder**, otomatikleştirilmiş istek fırlatma aracıdır. Çok sayıda payload’ı tek tek elle denemek yerine, **belirli bir alana sistematik olarak yüzlerce saldırı denemesi** yapılabilir. Hedef istek "Send to Intruder" ile aktarılır → parametre alanları seçilir → Payloadlar tanımlanır → Start attack.

