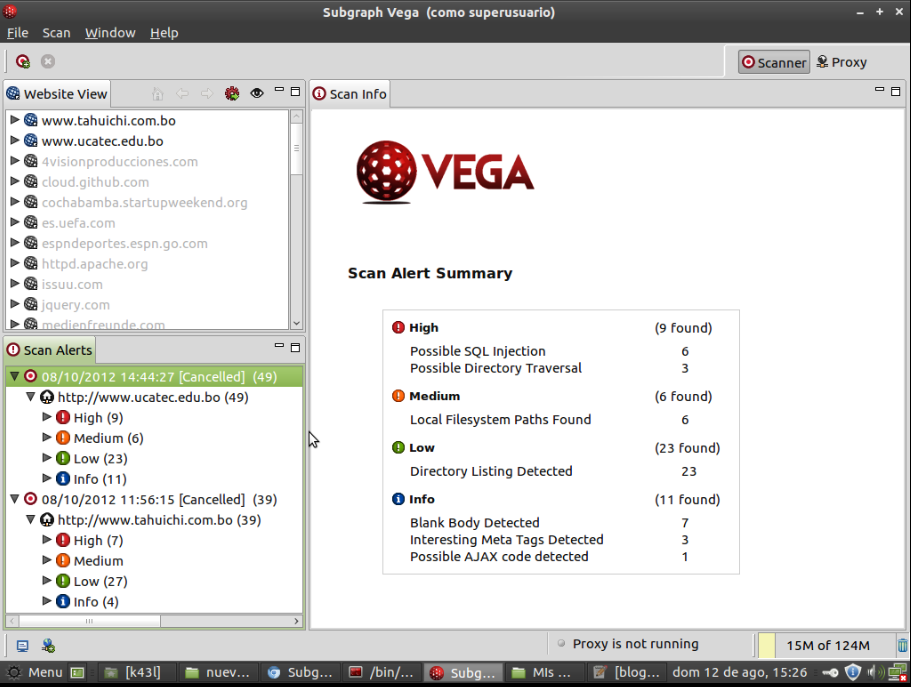
**Vega Nedir?**

Vega, Subgraph tarafından geliştirilen açık kaynaklı web uygulama güvenlik tarayıcısıdır. Java ile yazılmıştır ve grafikli arayüzü sayesinde Linux, Windows ve macOS’ta çalışabilir. Vega, SQL Injection, XSS gibi yaygın zafiyetleri otomatik olarak bulabilir ve aynı zamanda proxy özelliği ile manuel testlere de imkân tanır.



Vega açıldığında karşımıza çıkan ana ekran. Menü çubuğu, tarama başlatma seçenekleri ve alt araç sekmeleri bu ekrandadır. Yeni kullanıcılar için sezgisel bir yapıya sahiptir.

**Vega Nasıl Kurulur?**

Vega, Kali Linux gibi eğitim dağıtımlarında yüklü olabilir. Yoksa şu adımlarla kurulabilir:

***sudo apt update***

***sudo apt install libwebkitgtk-1.0-0 default-jdk unzip***

***wget https://support.subgraph.com/downloads/VegaBuild-linux.gtk.x86\_64.zip***

***unzip VegaBuild-linux.gtk.x86\_64.zip***

***cd vega***

***sudo ./Vega***

Bu sayede Java ve WebKit bağımlılıkları yüklenerek araç çalıştırılabilir.

**Vega ile Neler Yapabilirsiniz?**

* **Otomatik tarama:** Siteyi tarayarak link ve form parametreleri keşfeder.
* **Zafiyet tespiti:** SQLi, XSS, dosya içerik ifşası gibi güvenlik açıklarını analiz eder.
* **Intercepting proxy:** Tarayıcı-trafik üzerinde inceleme yapar ve güvenlik analizi sağlar.
* **Eklenti desteği:** JavaScript modüllerle özelleştirilebilir ve genişletilebilir.

**Vega Kullanımı – Temel Adımlar**

Terminalden veya GUI menüsünden “Vega” komutunu çalıştırın. İlk açılışta Scanner bakış açısı kullanıcıya sunulur.

**Yeni Tarama Başlatma (New Scan)**

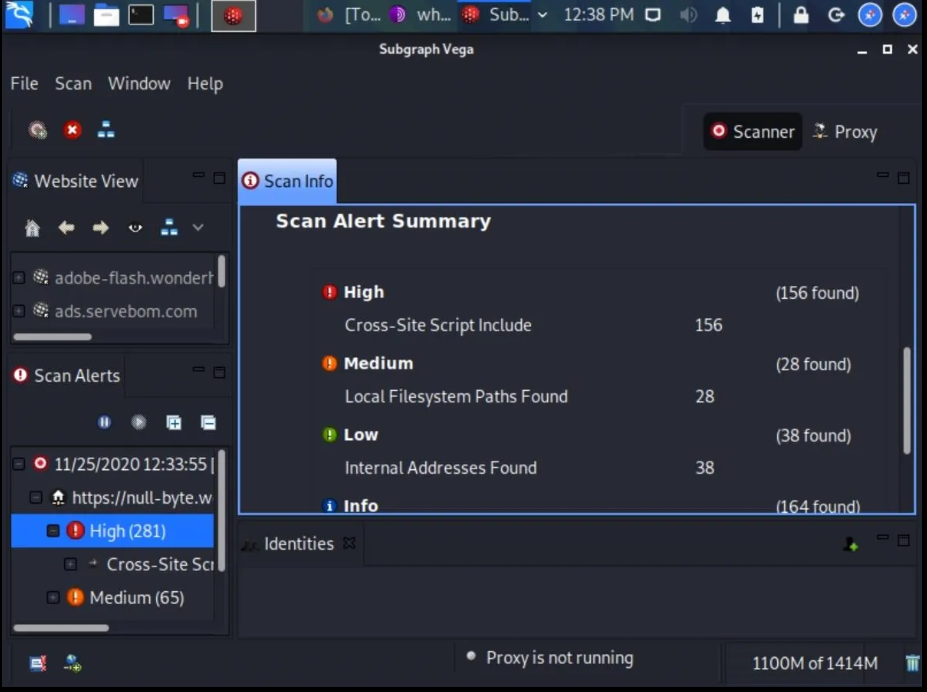
* **Add** tuşuna tıklayın, hedef URL’yi girin.
* İsterseniz tarama kapsamını (scope) belirleyebilirsiniz.

**Modülleri Seçin**

* **Injection modüller** (SQLi, XSS, LFI, RFI vb.)
* **Response modules** (cookie kontrol, kaynak kod ifşası algılama vb.)  
  Seçimi yaptıktan sonra tarama başlayabilir.

**4. Tarama Süreci ve Log Ekranı**

Tarama başladığında:



**Üst sol kısımda**, Vega’nın siteyi nasıl taradığını ve hangi URL’leri ziyaret ettiğini görebilirsiniz.

**Alt sol bölüm**, Vega’nın bulduğu güvenlik zafiyetlerini “High / Medium / Low” seviyelerinde sıralar.

**Sağ panel**, yapılan işlemler ve taramanın genel ilerlemesini gösterir.

* **Website View** paneli sol üstte aktif olur (linkler/form parametreler)
* **Scan Alerts** (sol alt) zafiyetleri listeler.
* **Scan Info** (sağ üst) tarama ilerlemesini grafiksel gösterir.

**Uyarı ve Detaylı İnceleme**

Tarama tamamlandığında:

* Zafiyetler **High/Medium/Low** olarak kategorize edilir.
* Her bir alert üzerine tıklayıp HTTP istek/yanıt, parametre bilgisi detaylı şekilde görülebilir [Null Byte](https://null-byte.wonderhowto.com/how-to/scan-websites-for-potential-vulnerabilities-using-vega-vulnerability-scanner-kali-linux-0181887/?utm_source=chatgpt.com).

Bu sayede yalnızca bulmak değil, anlamak da mümkün olur.

**Öğrencilere Tavsiyeler**

**Deneyin:** Kendinize ait bir test sitesi üzerinden (DVWA, Juice Shop gibi) tarama yapın.

**False positive’leri ayıklayın:** Yüksek uyarı her zaman gerçek açık anlamına gelmez; el yordamıyla kontrol edin.

**Proxy özelliği ile trafik analiz edin:** Manual testleri öğrenmek için harika bir seçenek.

**Kod yazın:** Kendi JavaScript modülünüzü oluşturup basit bir saldırıyı otomatik denetletebilirsiniz.

Vega, W3af gibi portföy araçlarının yanında kullanılan güçlü bir web güvenlik tarayıcısıdır. Otomatik ve yarı otomatik taramalarla hem hızlı hem de detaylı bulgu sağlayabilir. GUI arayüzü sayesinde özellikle grafik tabanlı öğrenciler için son derece uygundur.