**DOMinator**, istemci taraflı JavaScript tabanlı güvenlik açıklarını — özellikle **DOM tabanlı XSS (Cross-Site Scripting)** — tespit etmeye yardımcı olan gelişmiş bir **analiz aracıdır**. JavaScript kaynak kodunu analiz eder ve DOM manipülasyonları ile potansiyel zafiyetli noktaları gösterir.

DOMinator, özellikle JavaScript içinde geçen document.write(), innerHTML, location.hash, eval(), setTimeout(), document.URL gibi potansiyel tehlikeli API’lerin kullanımını takip eder.

**Bu Aracın Özellikleri Nelerdir?**

* **DOM Tabanlı XSS Analizi**: JavaScript içindeki potansiyel DOM XSS noktalarını tespit eder.
* **Statik Kod Analizi**: Otomatik olarak kaynak kodda şüpheli işlemleri gösterir.
* **Etkin Web Arayüzü**: Kullanımı kolay görsel arabirim sağlar.
* **Gelişmiş İzleme ve Haritalama**: Hangi girdilerin nereye ulaştığını gösterir.
* **Manuel ve Otomatik Tarama Desteği**.
* **Açık Kaynak**: GitHub üzerinden erişilebilir.

**DOMinator Aracını Kali Linux’a Kurma ve Kullanma Adımları**

**Adım 1: Gerekli Bağımlılıkları Kurun**

DOMinator, Python 2.7 ve pip gerektirir. Node.js de bazı modüller için gerekebilir.

“sudo apt install git python2 python2-pip nodejs -y”

**Adım 2: DOMinator Reposunu Klonlayın**

**“git clone https://github.com/SECFORCE/Dominator.git**

**cd Dominator”**

**Adım 3: Python Gereksinimlerini Kurun**

DOMinator dizinindeki requirements.txt dosyasını pip ile kurun.

“pip2 install -r requirements.txt”

**Adım 4: DOMinator’ı Başlatın**

“python2 DOMinator.py”

metin, ekran görüntüsü, yazı tipi, grafik içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 5: Web Arayüzüne Erişim Sağlayın**

Tarayıcıya şu adresi yazın: <http://localhost:8080>

**Adım 6: JavaScript Dosyasını Analiz Etme**

Web arayüzde “Upload File” veya “Enter URL” seçeneği ile bir .js dosyası yüklediğinizde DOM manipülasyonları analiz edilir.

Örnek taranan dosya :

“document.write(location.hash);”

DOMinator bunu tehlikeli olarak işaretler ve terminalde görünmez ama arayüzde vurgulu şekilde listelenir.