**CSRFTester**, web uygulamalarını **Cross-Site Request Forgery (CSRF)** saldırılarına karşı test etmek için kullanılan açık kaynaklı bir araçtır. OWASP tarafından geliştirilmiştir ve Java tabanlıdır. Bu araç, web uygulamanızın farklı formlarını analiz eder, potansiyel CSRF açıklarını belirler ve her form için saldırı senaryoları (exploit form) üretir.

Test sürecinde, uygulamanın CSRF token kullanıp kullanmadığını tespit eder ve zafiyet bulunan formlar için otomatik olarak **sahte HTML formları** oluşturur.

**Bu Aracın Özellikleri Nelerdir?**

* **CSRF Zafiyeti Tespiti**: Hedef web sayfalarında CSRF koruması olmayan formları bulur.
* **Exploit Üretimi**: Tespit edilen formlar için sahte form (HTML dosyası) üretir.
* **Manuel İnceleme**: Oluşturulan formlar tarayıcıda açılarak test edilebilir.
* **Basit ve Kullanıcı Dostu**: Web arayüzü ile form seçimi ve test süreci kolaydır.
* **Açık Kaynak**: OWASP tarafından geliştirildiği için güvenilir ve özgürce kullanılabilir.
* **Platform Bağımsız**: Java ile yazıldığı için Windows, Linux ve MacOS’ta çalışabilir.

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

**Adım 1: Java Kurulumunu Yapın**

CSRFTester Java ile çalıştığı için Java kurulu olmalıdır.

“sudo apt update

sudo apt install default-jdk -y”

**Adım 2: CSRFTester’ı İndirin**

GitHub üzerinden veya OWASP’in arşivinden CSRFTester’ı indirin:

“git clone https://github.com/OWASP/CSRFTester.git

cd CSRFTester”

**Adım 3: Uygulamayı Başlatın**

Proje klasörü içinde şu komutla Java uygulamasını çalıştırın:

“java -jar CSRFTester.jar”

Eğer CSRFTester.jar dosyası mevcut değilse, build klasörü altından çalıştırmanız gerekebilir:

“cd build

java -jar CSRFTester.jar”

Bu komut çalıştıktan sonra araç tarayıcınızda açılır.

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

Açıklama otomatik olarak oluşturuldu

**Adım 4: Web Arayüzüne Giriş Yapın**

Tarayıcıya şunu yazın:

<http://localhost:8008>

Varsayılan kullanıcı adı ve şifre:

* **Username**: admin
* **Password**: admin

**Adım 5: Test Edilecek Hedefi Ayarlayın**

1. Arayüzde “Target URL” kısmına test etmek istediğiniz web sayfasının adresini girin (örnek: http://192.168.1.10/profile.php).
2. “Start Test” butonuna tıklayın.

**Adım 6: Formlar Taranır ve Exploit Üretilir**

* Araç, sayfadaki HTML formları listeler.
* Hangi formlarda CSRF token olmadığı belirlenir.
* Zafiyet bulunan her form için bir **HTML saldırı formu (exploit.html)** oluşturulur.

Bu dosyayı tarayıcıda açtığınızda hedef uygulamaya karşı CSRF saldırısı yapılır.

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

Açıklama otomatik olarak oluşturuldu