**XSSer Nedir?**

**XSSer (Cross Site “Scripter”)**, web uygulamalarındaki **XSS (Cross-Site Scripting)** zafiyetlerini tespit etmek ve bu açıklıkları istismar etmek için kullanılan açık kaynak kodlu bir siber güvenlik aracıdır. Python diliyle yazılmıştır ve komut satırı üzerinden çalışır. XSSer, hem **Reflected XSS** hem de **Stored XSS** gibi birçok XSS türünü otomatik olarak algılayabilir ve test edebilir.

Bu araç, özellikle güvenlik araştırmacıları, etik hackerlar ve penetrasyon testi uzmanları için geliştirilmiştir. Farklı XSS payload'larını deneyerek uygulamalardaki açıkları test eder, bu sayede geliştiricilere zafiyetleri düzeltmeleri için yardımcı olur.

**XSS (Cross-Site Scripting) Nedir?**

XSS, saldırganların web uygulamalarına kötü amaçlı JavaScript kodu enjekte etmesine olanak tanıyan bir güvenlik açığıdır. Bu açık sayesinde:

* Oturum çerezleri çalınabilir,
* Kullanıcı tarayıcısında zararlı eylemler gerçekleştirilebilir,
* Phishing sayfaları görüntülenebilir.

XSS zafiyetleri, genellikle kullanıcıdan gelen verilerin düzgün filtrelenmemesi veya kaçırılmaması (escape edilmemesi) sonucu oluşur.

**XSS Türleri:**

1. **Reflected XSS:** Kullanıcının bir bağlantı aracılığıyla çalıştırdığı, anlık etki yaratan XSS türüdür.
2. **Stored XSS:** Zararlı kodun veritabanına kaydedildiği ve her ziyaretçide otomatik olarak çalıştığı XSS türüdür.
3. **DOM-Based XSS:** JavaScript ile istemci tarafında işlenen veriler üzerinden ortaya çıkan açıklardır.

XSSer, bu türlerin çoğunu test edebilecek donanıma sahiptir.

**XSSer’in Temel Özellikleri**

* **Farklı XSS Payload Desteği:** Aralarında basit alert() örneklerinden karmaşık DOM tabanlı kodlara kadar yüzlerce payload deneyebilir.
* **GET/POST Desteği:** URL parametrelerinin yanı sıra POST formlarını da tarayabilir.
* **DDoS Koruması Atlatma:** WAF ve güvenlik duvarlarını atlatmaya yönelik payload varyasyonları kullanır.
* **Proxy ve Tor Desteği:** Trafiği gizlemek için proxy ya da Tor ile kullanılabilir.

 **Form Analizi:** Sayfadaki formları otomatik tanır ve test eder.

 **Custom Payload:** Kullanıcının kendi özel saldırı yüklerini denemesine olanak tanır.

**Kurulum**

XSSer, Python 2 tabanlı bir araçtır. Kurulumu oldukça basittir:

**Debian/Ubuntu sistemlerde aşağıdaki komutlar sırasıyla yapılmalı:**

**sudo apt update**

**sudo apt install git python2**

**git clone https://github.com/epsylon/xsser.git**

**cd xsser**

**python2 xsser –help**

⚠️ Python 2 artık desteklenmiyor. Modern sistemlerde çalıştırmak için sanal ortam gerekebilir.

**XSSer’in Avantajları ve Dezavantajları**

**Avantajları:**

* Kullanımı kolaydır.
* Otomatik payload varyasyonları sayesinde hızlı test yapar.
* GET/POST/form desteğiyle kapsamlı analiz sağlar.
* Açık kaynak kodludur ve geliştirilebilir.
* Web arayüzü isteyenler için temel GUI desteği vardır.

**Dezavantajları:**

* Python 2 ile yazıldığı için güncel sistemlerde sorun yaşanabilir.
* DOM-Based XSS’yi her zaman doğru algılayamayabilir.
* Geliştirme desteği son yıllarda azalmıştır.
* CLI arayüzü yeni başlayanlar için zor olabilir.

**Gelin kullanımına beraber göz atalım:**

**metin, yazı tipi, ekran görüntüsü, bilgi, enformasyon içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**