**Yasuo Aracı Nedir?**

Yasuo, zayıf konfigüre edilmiş (yanlış yapılandırılmış) dosya yükleme açıklıklarını (file upload vulnerabilities) tespit etmeye yarayan bir güvenlik aracıdır. Genellikle penetrasyon testlerinde kullanılır. Dosya yükleme açıklıkları, saldırganların sisteme zararlı dosya yüklemesine izin veren ciddi bir güvenlik açığıdır. Yasuo bu açıklıkları tarar, analiz eder ve sistemde bu tür bir zaafiyet olup olmadığını belirler.

**Yasuo’nun Özellikleri**

* Web sunucularında dosya yükleme açıklıklarını tarar.
* Yükleme yollarını (upload path) ve uygulama cevaplarını analiz eder.
* Hızlı, basit ve kolay kullanılabilir bir komut satırı aracıdır.
* Ruby dili ile yazılmıştır.
* Genellikle diğer araçlarla birlikte kullanılarak detaylı analiz yapılabilir.

**Kullanım Alanları**

Yasuo’nun en çok kullanıldığı alanlar:

* Sızma Testleri (Penetration Testing)
* Zafiyet Taramaları (Vulnerability Assessment)
* Web Uygulama Güvenliği Analizi
* Siber Güvenlik Eğitimleri ve Laboratuvar Uygulamaları

**Kimler Kullanmalı?**

Yasuo’yu genellikle şu gruplar kullanır:

* Siber güvenlik uzmanları
* Penetrasyon testi yapanlar
* Siber güvenlik öğrencileri
* Güvenlik araştırmacıları

**Kurulum Aşaması (Adım Adım)**

**1.** Ruby'nin Kurulu Olduğundan Emin Ol

Yasuo, Ruby dili ile yazıldığı için sisteminde Ruby kurulu olmalı. Aşağıdaki komutla kurabilirsin: 

**2**. Git Kuruluysa Yasuo’yu Klonla: 

**3**. Klasöre Gir: 

**4.** Gerekli Ruby paketlerini yükle: 

Eğer bundle komutu yoksa şunu çalıştır: 

**5.** Aracı Çalıştır: 

Yukarıdaki komut, yardım menüsünü gösterir. Test etmek istediğin hedefleri ve dosyaları belirterek tarama yapabilirsin.

### ****Sonuç Olarak:****

Yasuo, web uygulamalarındaki dosya yükleme açıklarını bulmak için geliştirilmiş hafif, hızlı ve etkili bir araçtır. Özellikle güvenlik araştırmacılarının ellerinde güçlü bir yardımcıdır. Kurulumu kolay ve kullanımı anlaşılırdır. Ancak doğru sonuçlar alabilmek için temel siber güvenlik bilgisi gereklidir.