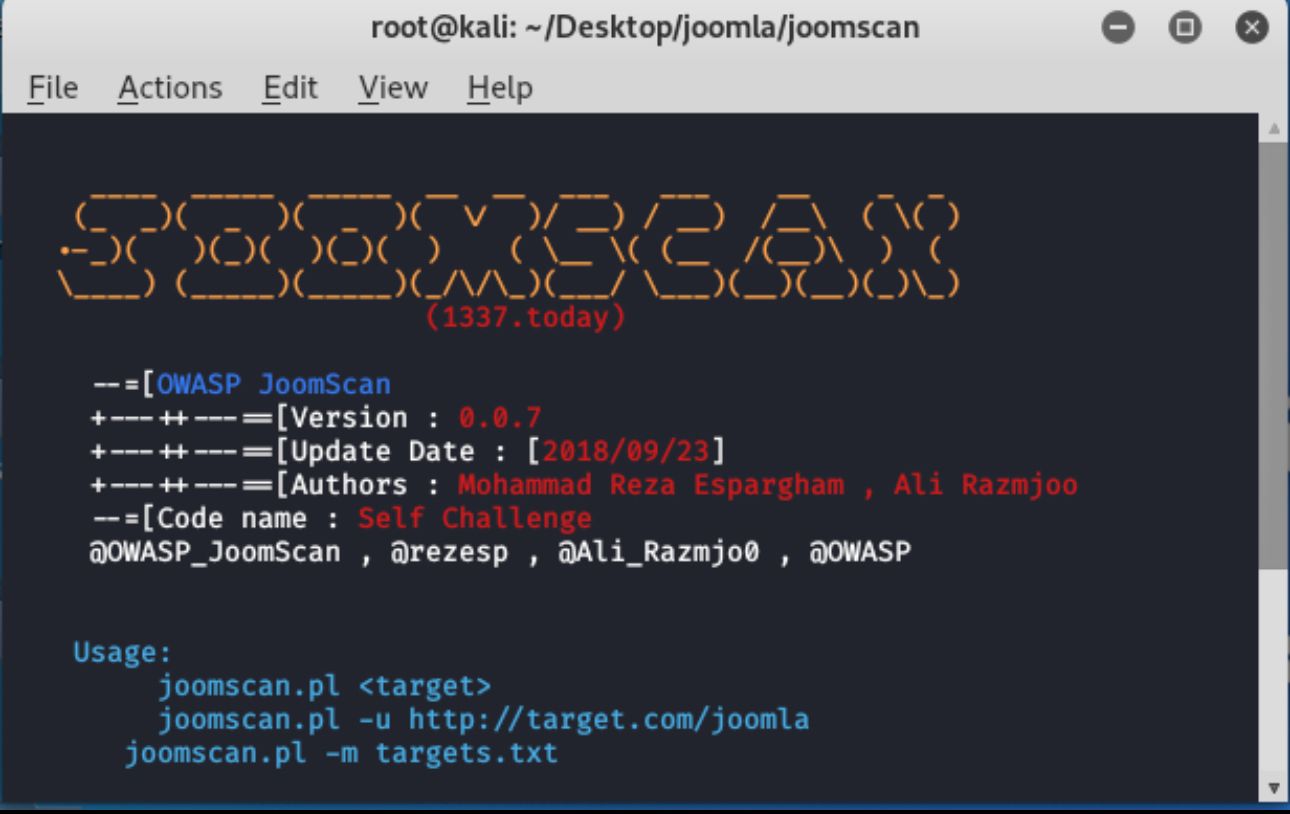
**JoomScan Nedir?**

JoomScan, **Joomla** içerik yönetim sistemi (CMS) kullanan web sitelerindeki güvenlik açıklarını tespit etmek için geliştirilmiş açık kaynaklı bir güvenlik aracıdır. PHP ile yazılmıştır ve özellikle Joomla sitelerinde bulunan bilinen zafiyetleri hızlıca bulup raporlamak için kullanılır.

**JoomScan Ne İşe Yarar?**

* Joomla sürümünü ve kurulu bileşenleri (plugin, modül, tema) tarayarak güvenlik zafiyetlerini bulur.
* Bilinen Joomla açıklarını ve hatalı yapılandırmaları tespit eder.
* Site güvenliğini test etmek için pentesterlar tarafından sık kullanılır.
* Otomatik olarak Joomla sürüm bilgisi çekebilir, güvenlik açığı veritabanını kontrol eder.

**JoomScan Nasıl Kurulur?**

****

JoomScan genellikle Kali Linux ve diğer pentest dağıtımlarında hazır gelir. Eğer sisteminizde yoksa şu şekilde kurabilirsiniz:

***git clone https://github.com/rezasp/joomscan.git***

***cd joomscan***

***chmod +x joomscan.pl***

Perl dili ile çalışır, bu yüzden sistemde Perl kurulu olmalıdır (çoğu Linux dağıtımında varsayılan olarak kurulu gelir).

**JoomScan Nasıl Kullanılır?**

Basit bir komut satırı aracı olduğu için terminalden kolayca kullanabilirsiniz.

**Temel Tarama Komutu:**

***perl joomscan.pl -u*** [***https://hedef-site.com***](https://hedef-site.com)

**Burada -u parametresi ile taranacak Joomla sitesinin URL’si verilir.**

**JoomScan’in Öne Çıkan Özellikleri:**

**Sürüm Tespiti:** Joomla sürümünü belirler.

**Açık Taraması:** Bilinen Joomla çekirdek, bileşen, tema ve modül açıklarını tarar.

**Dosya ve Dizin Kontrolü:** Hassas dosya/dizinlerin erişilebilir olup olmadığını test eder.

**Güvenlik Tavsiyeleri:** Tarama sonunda bulunabilecek zafiyetler için çözüm önerileri verir.

**Raporlama:** Konsola detaylı rapor sunar, istenirse çıktı dosyasına kaydedilebilir.

**JoomScan Kullanımı – Temel Adımlar**

Terminali açın ve JoomScan dizinine gidin.

Aşağıdaki gibi tarama başlatın:

***perl joomscan.pl -u*** [***https://hedef-site.com***](https://hedef-site.com)



Tarama başladığında konsolda Joomla sürümü, tespit edilen açıklar, erişilebilir dosyalar listelenir.

Tarama sonunda bulunan kritik ve orta dereceli güvenlik zafiyetleri detaylı şekilde gösterilir.



**Öğrencilere Tavsiyeler**

* Kendi lokal Joomla test ortamınızı (örneğin Bitnami Joomla veya XAMPP ile) kurarak JoomScan ile tarama yapın.
* Tarama sonuçlarını dikkatle inceleyin ve “false positive” olabilecek sonuçları ayıklayın.
* Bulunan açıkları anlamak için Joomla’nın nasıl çalıştığını ve zafiyetlerin nasıl oluştuğunu öğrenin.
* JoomScan’ı diğer pentest araçları (örneğin Nikto, WPScan gibi) ile kombine kullanarak kapsamlı analiz yapın.

**JoomScan Kullanırken Dikkat Edilmesi Gerekenler**

* Yalnızca **izin verilen sistemlerde** test yapınız. Yetkisiz taramalar yasa dışıdır.
* Tarama sırasında hedef sistemde aşırı yük oluşabilir, performans sorunlarına neden olabilir.
* Araç çıktılarında bulunan tüm açıklar her zaman gerçek olmayabilir, elle doğrulama önemlidir.

JoomScan, Joomla tabanlı web uygulamalarını hızlı ve etkili şekilde analiz etmek için ideal bir araçtır. Hem otomatik tarama hem de detaylı raporlama özellikleriyle, web uygulaması güvenlik testlerinde vazgeçilmezdir.