Semgrep Aracı - Eğitim Materyali

# 🧠 Semgrep Nedir?

Semgrep, kaynak kodunda güvenlik açıklarını, stil hatalarını ve kötü uygulamaları tespit etmeye yarayan hafif, hızlı ve açık kaynaklı bir statik analiz aracıdır.  
SAST (Static Application Security Testing) kategorisinde yer alır ve Python, JavaScript, Go, Java, C, C++, PHP, Ruby, YAML gibi birçok dili destekler.

# 🚀 Özellikleri

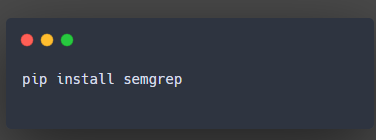
- Hızlı ve dosya seviyesinde statik analiz  
- Ön tanımlı ya da özel kural setleriyle çalışabilir  
- CI/CD hatlarına kolay entegrasyon (GitHub Actions, GitLab, Jenkins)  
- Çok sayıda dil desteği ve özel kurallar yazabilme  
- Kurallar Semgrep Registry'den indirilebilir veya manuel yazılabilir

# 🎯 Kullanım Alanları

- Güvenlik açığı tespiti (XSS, SQLi, SSRF, vs.)  
- Kod kalitesi ve kod standardı analizi  
- Güvenli yazılım geliştirme eğitimleri  
- Kodda parola, token, API anahtarı gibi hassas veri sızıntılarını önleme

# 🛠️ Kurulum

1. pip ile yükleme (Python yüklü ise):

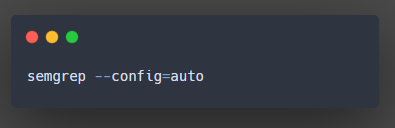
******

2. ya da doğrudan binary ile:

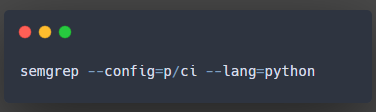
# 

# 🧪 Örnek Semgrep Komutları ve Açıklamaları

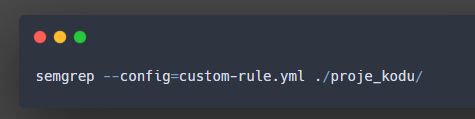
✅ 1. Tüm Projeyi Varsayılan Kurallarla Tara:

******

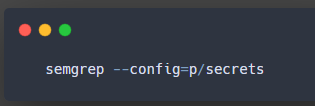
✅ 2. Python İçin CI Güvenlik Kuralları:

******

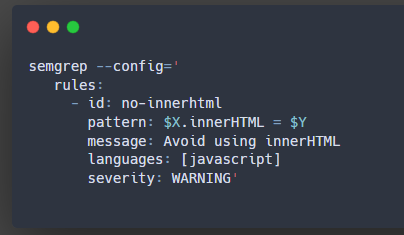
✅ 3. Özel Yazılmış YAML Kuralları ile Tarama:

******

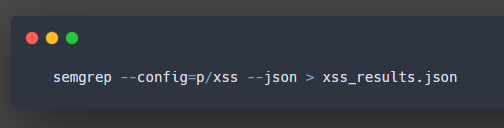
✅ 4. Parola ve Token Sızıntısı Tespiti:

******

✅ 5. JavaScript’te innerHTML Kullanımını Tespit Et:

******

✅ 6. XSS Tespiti ve JSON Raporu Oluşturma:

******

✅ 7. Kodda eval() veya exec() Kullanımı Tespiti:

# 

# 📎 Notlar

- Semgrep Registry'de 2000+ hazır kural mevcuttur: https://semgrep.dev/explore  
- Kurallar YAML ile yazılır; `pattern`, `message`, `severity` gibi alanlar içerir.  
- Kod güvenliği eğitimlerinde öğrencilere kendi kurallarını yazdırmak mümkündür.  
- JSON, SARIF ve JUNIT gibi çıktılar desteklenir.