**DUMPSTERDİVER**

**DumpsterDiver Nedir?**

DumpsterDiver, yazılım projelerinde veya dosya sistemlerinde saklı kalmış API anahtarları, parolalar, gizli tokenlar gibi hassas bilgileri tespit etmek için kullanılan bir açık kaynak güvenlik aracıdır. Özellikle arşivlenmiş dosyaları (zip, tar vb.) da tarayabilmesiyle öne çıkar.

**Özellikleri:**

✓Arşiv dosyalarını tarama: ZIP, TAR gibi sıkıştırılmış dosyalarda gizli verileri bulabilir.

✓Regex tabanlı tarama: Özel desenlerle kişiselleştirilmiş tarama yapılabilir.

✓Hızlı çalışma: Büyük projelerde bile etkili sonuçlar verir.

✓JSON raporlama: Bulunan sonuçları JSON formatında raporlar.

✓Platform bağımsız: Python tabanlı olduğu için Windows, Linux ve macOS’ta çalışır.

**Kullanım Alanları:**

•Kod depolarında kazara bırakılmış gizli bilgileri tespit etme.

•Penetrasyon testlerinde veri sızıntısı risklerini belirleme.

•CI/CD süreçlerinde otomatik güvenlik denetimi sağlama.

•Şirket içi güvenlik taramalarında manuel denetim yükünü azaltma.

**Kurulum Aşamaları:**

**– Git ve Python kullanarak**

**1**. Python 3 kurulu olduğundan emin olun.

**2**. Depoyu klonlayın: 

**3**. Dizine girin:



**4**. Gerekli paketleri yükleyin: 

**5**. Aracı çalıştırın: 

**Dikkat Edilmesi Gerekenler:**

✓Çok büyük projelerde tarama süresi uzayabilir; işlem öncesinde filtreleme yapılabilir.

✓Özel regex kuralları dikkatle hazırlanmalı, aksi takdirde yanlış pozitif sonuçlar çıkabilir.

✓Tarama sonucunda bulunan gizli bilgilerin güvenliği sağlanmalı ve erişim yetkileri sınırlandırılmalı.

✓Kullanım sırasında sistem kaynaklarını zorlayabileceğinden paralel işlemler planlanmalıdır.