**SecLists Nedir?**

SecLists, siber güvenlik uzmanları tarafından kullanılan kelime listelerinin (wordlists) büyük bir koleksiyonudur. Özellikle sızma testleri (penetration testing) ve web güvenliği testlerinde kullanılır.

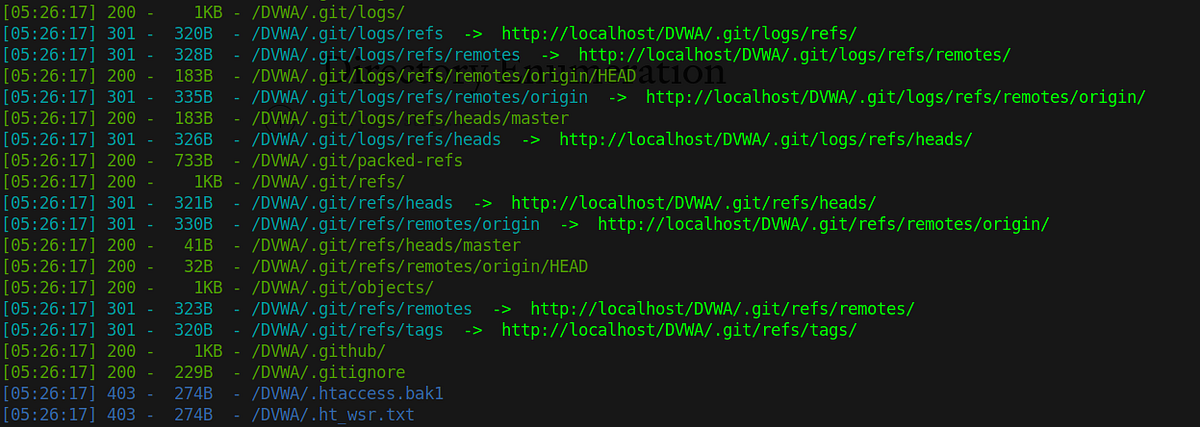
Basitçe anlatmak gerekirse:

SecLists, güvenlik testleri sırasında ihtiyaç duyduğumuz kullanıcı adı, parola, URL, dizin adı gibi hazır listeleri içinde barındıran bir araç değil, bir veri koleksiyonudur.

**Ne İşe Yarar?**

SecLists genellikle şu alanlarda kullanılır:

* **Brute force saldırıları**: Kullanıcı adı ve şifre denemelerinde kullanılır. Örneğin, bir sistemde zayıf şifrelerin denenmesi için hazır parola listeleri sağlar.
* **Dizin keşfi**: Web sitelerinde gizlenmiş klasör ve dosyaları bulmak için kullanılır. Özellikle web uygulaması güvenliğini test etmekte yaygındır.
* **Fuzzing**: Web uygulamalarına farklı türlerde veriler göndererek açıklara karşı nasıl tepki verdiği test edilir.
* **Payload testleri**: SQL Injection, XSS gibi güvenlik açıklarını test etmek için hazır saldırı verileri içerir.
* **Sosyal mühendislik testleri**: E-posta adresleri, kullanıcı adları ve isim-soyisim gibi bilgilerle yapılan testlerde kullanılabilir.



SecLists’in bir dizin keşfi (directory enumeration) sırasında kullanıldığını gösteren ekran, wordlist dosyasının işlendiği ve sonuçların terminalde çıktığı örnek.

**SecLists Nasıl Kurulur?**

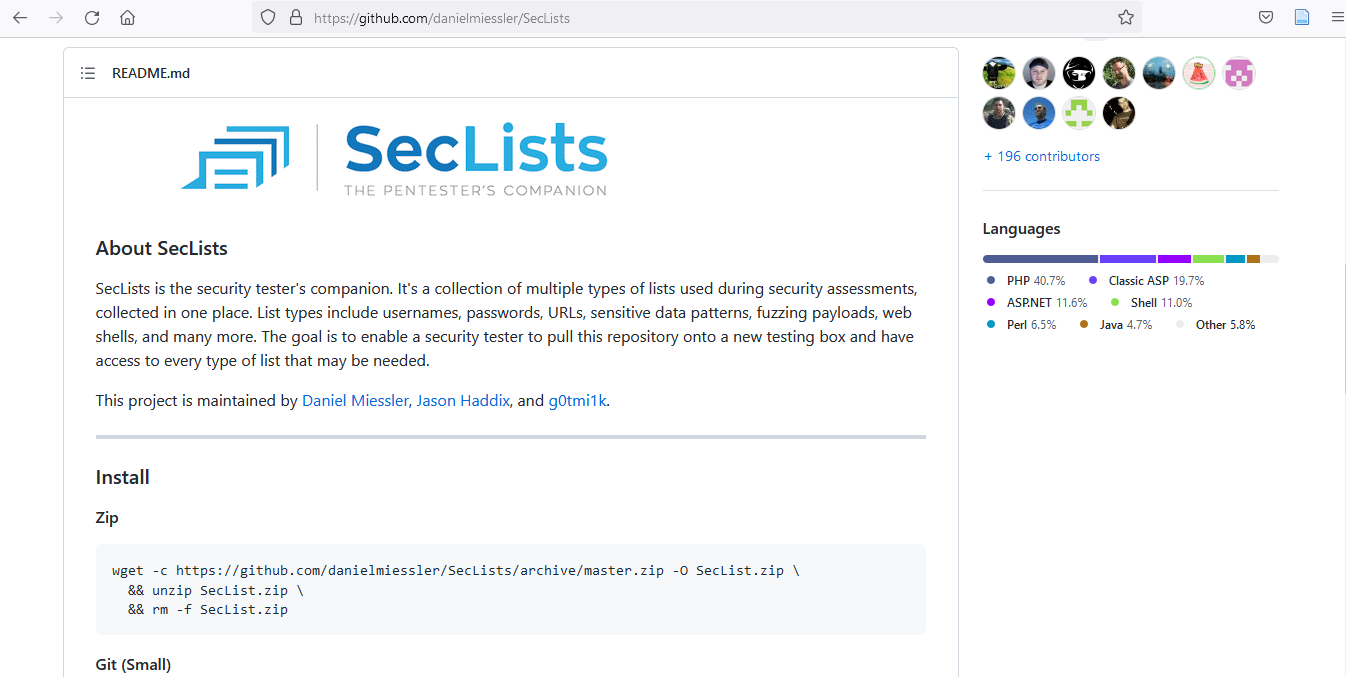
Git ile Yükleme:

SecLists GitHub’da barındırılır. Kurmak yerine genellikle sadece indirilir:

***git clone https://github.com/danielmiessler/SecLists.git***

İndirdikten sonra SecLists klasörünün içinde şu başlıca dizinler bulunur:

* SecLists/
* Discovery
* Passwords
* Fuzzing
* Web-Shells
* Usernames
* Payloads
* Miscellaneous



SecLists klasör yapısı: Discovery, Passwords, Fuzzing, Payloads gibi alt klasörlerin terminalde nasıl listelendiğini gösteren ekran.

**Avantajları ve Dikkat Edilmesi Gerekenler**

**Avantajları**

* Açık kaynak ve tamamen ücretsiz
* Çok geniş kullanım alanı
* Saldırılar için zaman kazandırır (hazır veriler)
* Sürekli güncellenmektedir

**Dikkat Edilmesi Gerekenler**

* Kendi başına bir araç değildir, veri koleksiyonudur
* Gerçek sistemlere karşı izinsiz kullanım yasaktır
* Her zaman sanal makinede veya yasal test ortamında kullanılmalıdır

**SecLists**, siber güvenlik testlerinde kullanılmak üzere hazırlanmış en kapsamlı kelime listesi ve test verisi koleksiyonudur. Öğrenciler, bu listeyi kullanarak:

* Güvenlik açıklarını test etmeyi
* Brute force saldırılarını anlamayı
* Web uygulaması güvenliğini değerlendirmeyi öğrenebilirler.

Gerçek saldırılarda kullanılan yöntemleri güvenli ve kontrollü bir ortamda öğrenmenin en etkili yöntemidir.