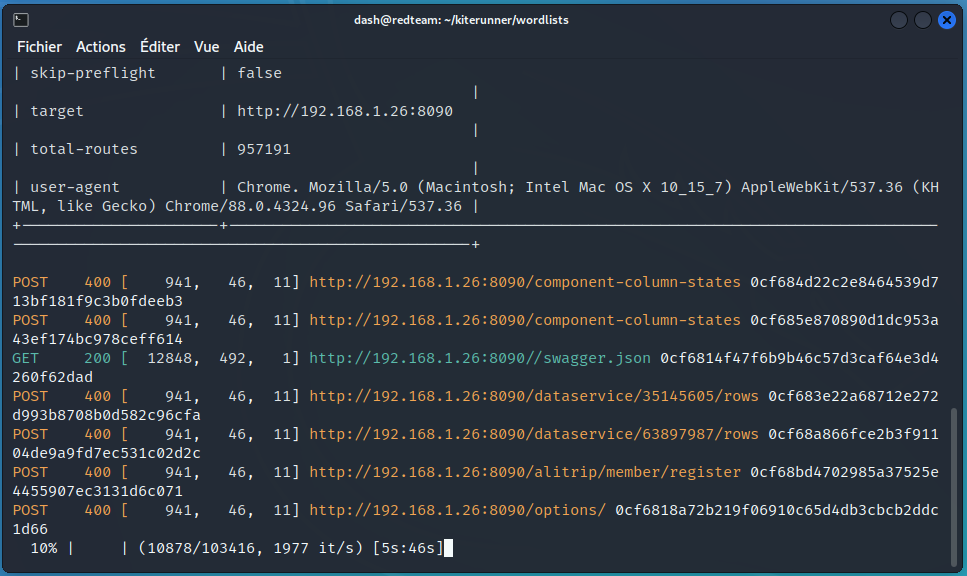
**Kiterunner Nedir?**

Kiterunner, API odaklı web uygulamalarında endpoint keşfi (API fuzzing) yapmak için geliştirilmiş açık kaynaklı bir araçtır.  
Burp Suite veya klasik dizin tarayıcılar (Dirb, Gobuster, ffuf) gibi araçlar, genellikle web dizinlerini tararken; Kiterunner, OpenAPI/Swagger gibi API şemalarını da analiz edebilir ve REST API uç noktalarına özgü keşifler yapabilir.

Kiterunner, Go dilinde yazılmıştır ve hızlıdır. Ayrıca büyük kurumsal uygulamalarda bile etkili şekilde çalışabilir.

**Kiterunner Ne İşe Yarar?**

* Web uygulamalarında kullanılan REST API uç noktalarını keşfeder.
* API endpoint’lerine parametreli istekler göndererek cevapları analiz eder.
* Swagger (OpenAPI) dosyalarını kullanarak hedefli ve akıllı tarama yapar.
* API üzerindeki HTTP metotlarını (GET, POST, PUT, DELETE) test eder.
* Belirli HTTP durum kodlarına göre filtreleme ve sıralama yapabilir.



**Kurulum:**

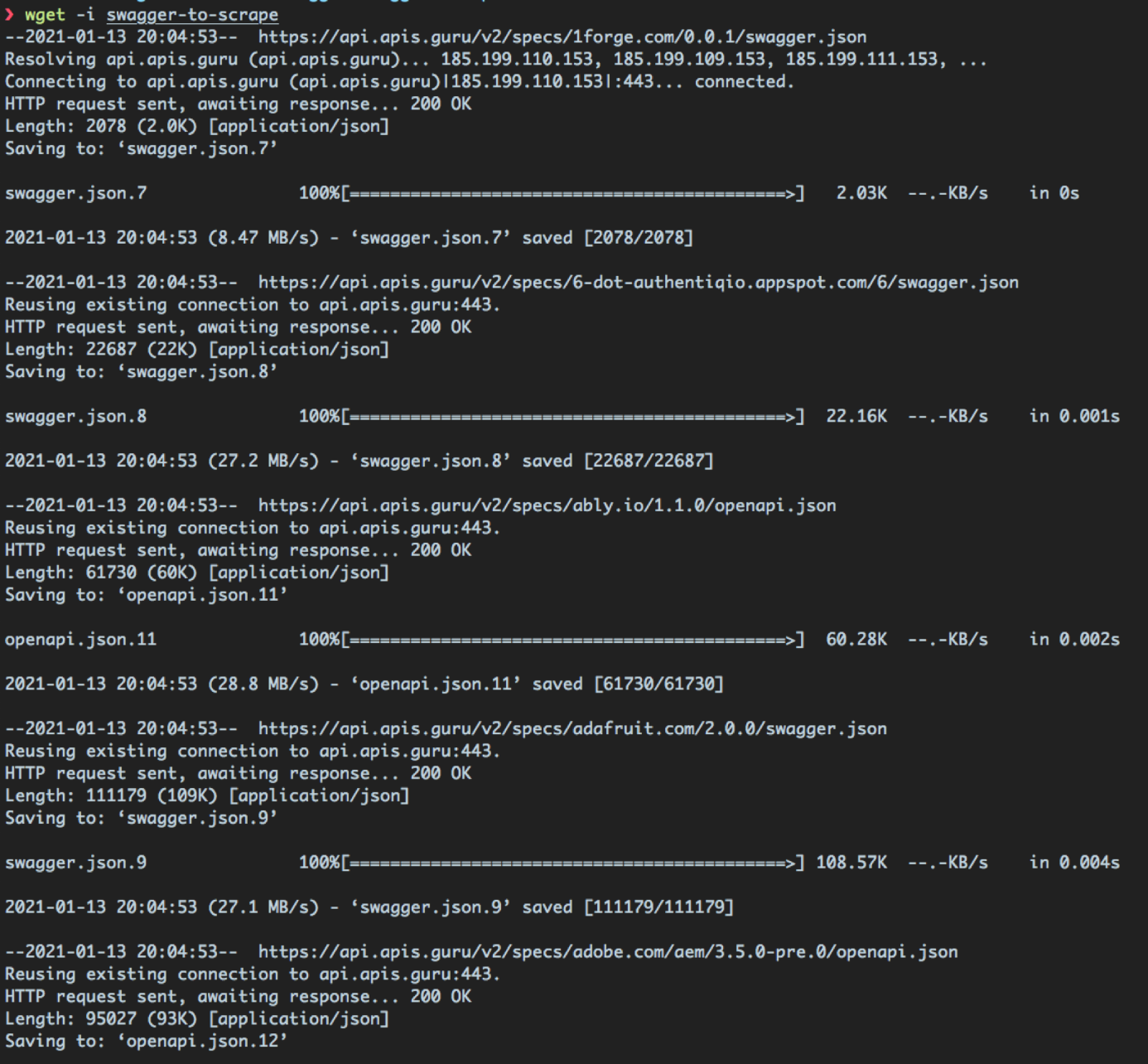
***git clone https://github.com/assetnote/kiterunner.git***

***cd kiterunner***

***make build***

İkili dosya (binary) oluştuktan sonra ***./dist/kr*** ile çalıştırılabilir.

Kiterunner, Assetnote’un sağladığı özel wordlist’lerle (routes-large.kite gibi) birlikte kullanıldığında çok etkilidir.



Basic API Scan” komut sonrası kullanılan wordlist'ler ve taranan endpoint’lerin detaylı çıktıları terminalde listeleniyor.

**Temel Kullanım Komutları**

1. Basit endpoint keşfi:

***./kr scan https://hedefapi.com -w routes-large.kite***

1. OpenAPI şeması üzerinden tarama:

***./kr scan https://hedefapi.com --openapi openapi.json***

1. Sadece 200 ve 403 durum kodlarını filtrele:

***./kr scan https://hedefapi.com -w routes.kite -s 200,403***

1. Çıktıyı dosyaya yazmak:

**./kr scan https://api.example.com -w routes.kite -o result.txt**

Kiterunner, klasik dizin tarayıcılarının ötesine geçerek modern uygulamalarda yaygınlaşan RESTful API'lerin saldırı yüzeyini ortaya çıkartır. Bu araç, bilinen endpoint’lere değil, tahmin edilebilir veya Swagger dosyasına dahil edilmiş endpoint’lere istek göndererek daha hedefli bir keşif süreci yürütür.

Ayrıca, Kiterunner’ın kullandığı .kite uzantılı wordlist'ler, yalnızca endpoint adlarını değil, bu endpoint’lerde denenebilecek HTTP metotlarını da içerir. Bu sayede hem endpoint’in varlığı test edilir hem de bu endpoint’te hangi HTTP metotlarının çalıştığı öğrenilir.

Diğer tarama araçlarıyla kıyaslandığında, daha az false positive ve daha fazla isabetli sonuç sunar.