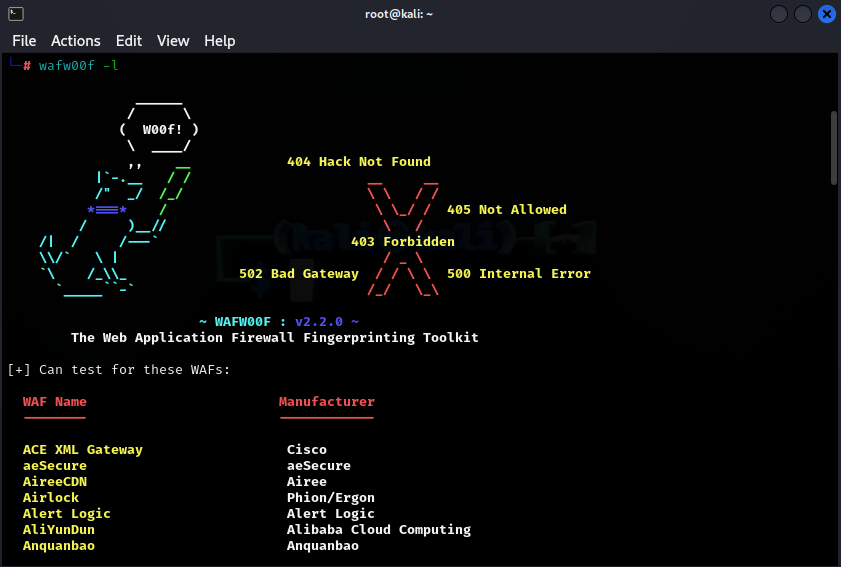
**Wafw00f Tool Nasıl Çalışır?**

* Normal bir HTTP isteği gönderir ve yanıtı analiz eder; bu, bir dizi WAF çözümünü tanımlar.
* Bu başarılı olmazsa, bir dizi (potansiyel olarak kötü amaçlı) HTTP isteği gönderir ve bunun hangi WAF olduğunu anlamak için basit bir mantık kullanır.
* Bu da başarılı olmazsa, daha önce gönderilen yanıtları analiz eder ve bir WAF veya güvenlik çözümünün saldırılarımıza aktif olarak yanıt verip vermediğini tahmin etmek için başka bir basit algoritma kullanır.

**Wafw00f**tolunun hangi WAF’ları tespit ettiğini görmek istersek aşağıdaki komutu çalıştırabiliriz.

wafw00f -l



Yukarıda gördüğümüz gibi bir çok WAF tespitini yapabiliyor. Liste oldukça uzun olduğu için ben tamamını buraya eklemedim. Detaylı görmek için komutu çalıştırarak inceleyebilirsiniz.

**Wafw00f Kurulumu**

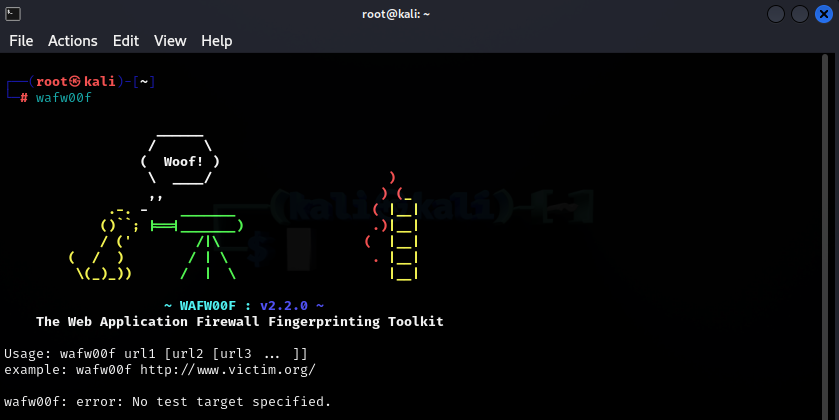
Araç **kurulumu**nu yapmak için aşağıda yer alan github adresine giderek komutu kullanarak kendi sistemimize indiriyoruz.

**git clone https://github.com/EnableSecurity/wafw00f**

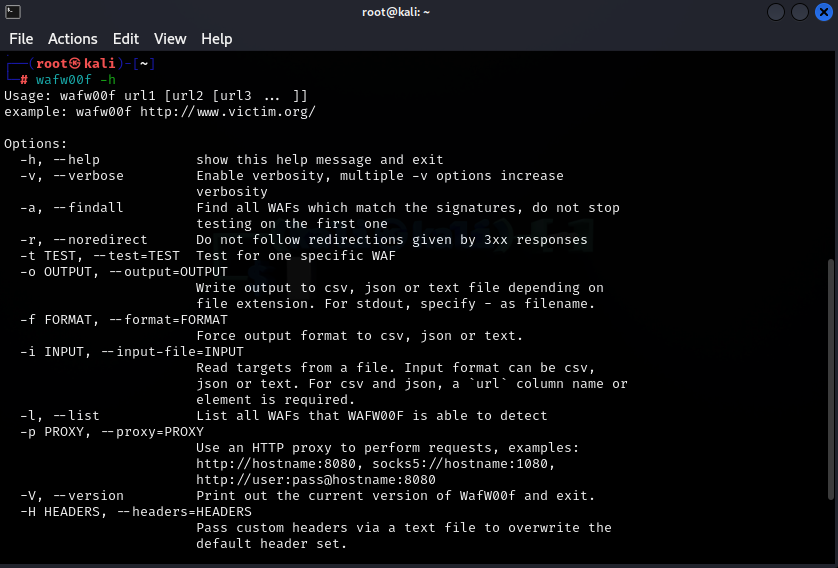
Daha sonra **wafw00f tool**u ile aynı dizine gelip aşağıdaki komutu çalıştırıyoruz.

**python setup.py install**

Bu şekilde kurulum tamamlanmış oluyor. Kontrol edelim.

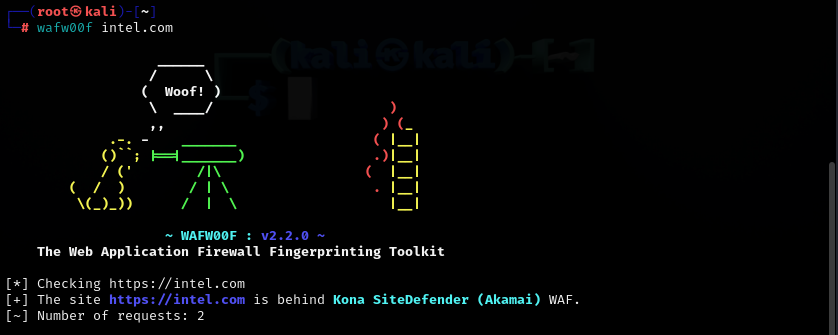
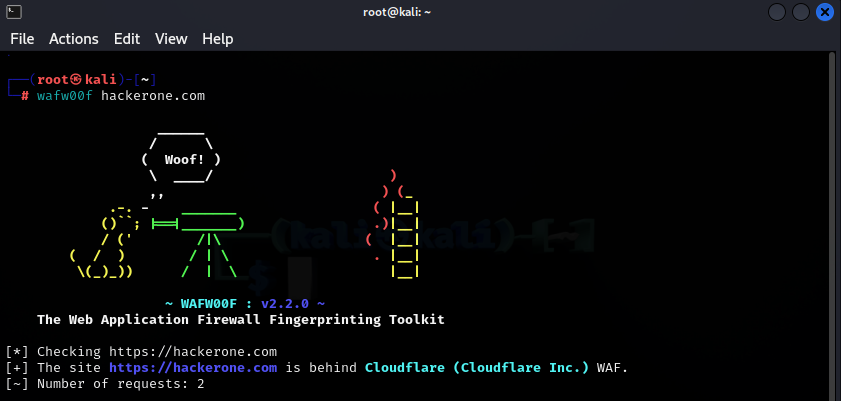


Wafw00f sistemimize başarılı bir şekilde kuruldu. Help komutu ile neler yapabileceğimizi inceleyelim.



**Wafw00f Kullanımı**

Wafw00f tool kullanımı çok kolay bir araçtır. **Wafw00f ile bir tarama** yaparak sonuçlarına bakalım.



Yukarıda görüldüğü üzere 2 adet örnek hedefe bir tarama gerçekleştirdik ve WAF olarak Cloudflare ve Kona SiteDefender kullanıldığını tespit ettik.

Web testlerinde firewall tespit ederek ne tür bir aksiyon alacağımızı belirlemek için kullanışlı ve kullanımı basit bir tool. Bug bounty ve pentestlerde sıklıkla kullanılmaktadır.