wafw00f Nedir?

wafw00f, bir hedef web sitesinin önünde bir WAF (Web Application Firewall) olup olmadığını tespit eden bir bilgi toplama aracıdır. Eğer varsa, hangi WAF’ın kullanıldığını da belirtmeye çalışır.

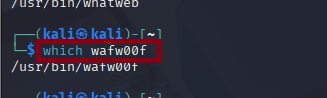
wafw00f Özellikleri

* **WAF tespiti yapar:** Hedef web uygulamasının bir WAF arkasında olup olmadığını belirler.
* **WAF türünü tanımlar**: Cloudflare, Akamai, F5 BIG-IP, AWS WAF, ModSecurity gibi birçok popüler güvenlik duvarını tanıyabilir.
* **Pasif tarama yöntemi kullanır:** Web sitesine zarar vermeden yalnızca HTTP istekleriyle çalışır.
* **Geniş test dizisine sahiptir:** Farklı türde HTTP istekleri göndererek WAF davranışlarını analiz eder.
* **Toplu hedef taraması yapabilir:** Birden fazla hedefi dosya üzerinden sırayla tarayabilir (-r parametresi ile).
* **Komut satırı (CLI) ile çalışır:** Terminal üzerinden kolayca kullanılabilir ve otomasyon sistemlerine entegre edilebilir.
* **Verbose (ayrıntılı) mod desteği vardır:** Tarama sürecini detaylı olarak izleme imkânı sunar.
* **False positive oranı düşüktür:** Yüksek doğruluk oranıyla çalışır.
* **HTTPS desteği mevcuttur:** Hem HTTP hem de HTTPS sitelerle sorunsuz çalışır.

Kali Linux'ta wafw00f Kurulumu

Kali Linux’ta genellikle önceden kurulu gelir. Emin olmak için terminale şu komutu yaz:

which wafw00f



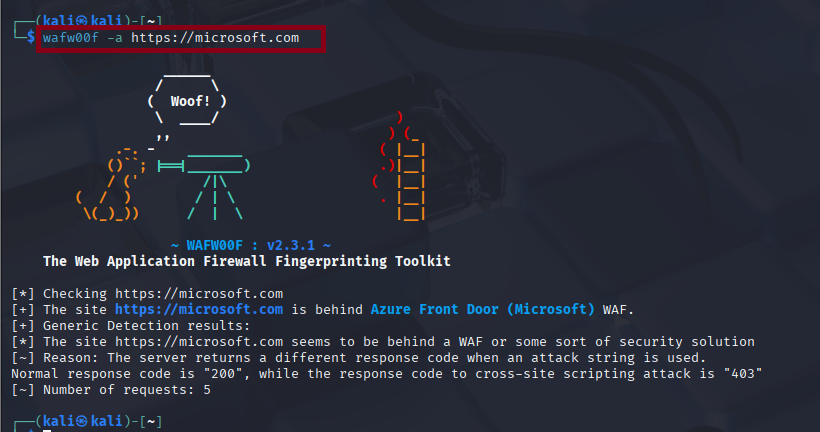
Aksi hâlde kurmak için:

sudo apt update

sudo apt install wafw00f

Temel Kullanımı

wafw00f -a <https://microsoft.com>



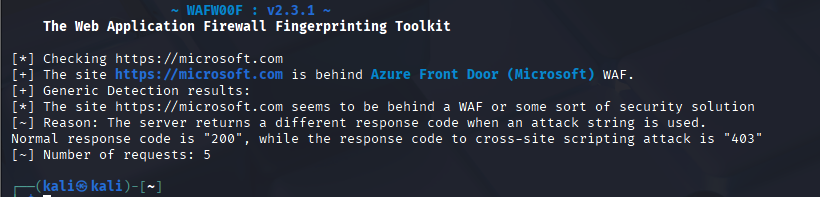
Açıklaması:

wafw00f: Aracı başlatır.

-a: Tüm tespit testlerini uygular (a: aggressive / all tests). Daha detaylı analiz yapılmasını sağlar.

https://microsoft.com: Hedef web sitesi. Bu örnekte Microsoft’un ana domaini analiz ediliyor.

Çıktının Açıklaması



1 Checking https://microsoft.com

Hedef olarak belirttiğimiz siteye bağlantı başlatılıyor.

2 The site https://microsoft.com is behind Azure Front Door (Microsoft) WAF.

Site, Azure Front Door adlı WAF (Web Application Firewall) arkasında korunuyor.

Bu, Microsoft’un gelişmiş güvenlik altyapısı kullandığını gösterir.

3 Generic Detection results:

Genel bir WAF tespit analizine geçiliyor.

Bu bölüm, tespit detaylarını içerir.

4 The site seems to be behind a WAF or some sort of security solution

wafw00f, bu sitenin yalnızca WAF değil, olası başka bir güvenlik önlemiyle de korunduğunu belirtiyor.

5 The site seems to be behind a WAF or some sort of security solution

wafw00f, bu sitenin yalnızca WAF değil, olası başka bir güvenlik önlemiyle de korunduğunu belirtiyor.

6 Normal response code is "200", while the response to cross-site scripting attack is "403"

200: Normal sayfa başarıyla döndü.

403: XSS (Cross-Site Scripting) gibi zararlı bir istek gönderildiğinde erişim engellendi.

Bu davranış, aktif bir WAF’ın göstergesidir.

7 Number of requests: 5

Tespitte toplam 5 farklı istek kullanılmı