**🧠 1. WafW00f Nedir?**

**WafW00f**, bir web uygulamasının arkasında **WAF (Web Application Firewall)** olup olmadığını tespit eden bir komut satırı aracıdır.

📌 Amaç:

* Hedef siteye bir WAF koruması uygulanıp uygulanmadığını belirlemek
* Hangi marka/model WAF kullanıldığını anlamak
* Pentest öncesi WAF bypass stratejileri planlamak

**🧠 2. Web Application Firewall (WAF) Nedir?**

**WAF**, web trafiğini filtreleyen ve zararlı istekleri engelleyen bir güvenlik katmanıdır.  
SQLi, XSS, RFI gibi saldırıları engellemek amacıyla kullanılır.

📌 Yaygın WAF örnekleri:

* Cloudflare
* AWS WAF
* Imperva
* F5 BIG-IP
* Sucuri
* Akamai

**🎯 3. WafW00f Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🔍 WAF olup olmadığını tespit eder | Pasif ve aktif teknikler kullanır |
| 🛡️ WAF markasını belirler | 80+ farklı WAF ürününü tanır |
| ⚙️ HTTP cevaplarına göre analiz | Header, response code ve davranışa göre tespit yapar |
| 🧪 Bypass için ön analiz sağlar | Teste başlamadan önlem alınmasını kolaylaştırır |

**⚙️ 4. Kurulum (Kali / Linux)**

**✅ Python ile (kaynak koddan):**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🚀 5. Kullanım Komutları**

**✅ Temel kullanım:**

wafw00f https://targetsite.com

**✅ Detaylı çıktı ile tarama:**

wafw00f https://targetsite.com -a

**✅ Dosya içinden çoklu hedef tarama:**

wafw00f -i targets.txt

**📋 6. Örnek Terminal Çıktısı**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🧠 7. WafW00f Tespit Yöntemleri**

| **Yöntem** | **Açıklama** |
| --- | --- |
| 📥 HTTP response analizi | Status kodlar, header’lar, içerik değişimi |
| 🧬 Signature tabanı | Belirli WAF’lere ait imzalar |
| 💣 Test payload’lar | XSS, SQLi gibi zararlı isteklerle sistem davranışı test edilir |
| 🔍 Rate-limit, captchas | WAF davranışları gözlemlenir |

**📊 8. WafW00f ile Tespit Edilebilen Bazı WAF Ürünleri**

* Cloudflare
* AWS WAF
* Akamai
* Barracuda
* F5 BIG-IP
* Fortinet
* Imperva Incapsula
* Microsoft Azure
* Citrix NetScaler
* Sucuri
* ModSecurity
* URLScan

(Toplam 80+ tanımlı WAF)

**🛡️ 9. Neden Önemlidir?**

* 🔍 WAF tespiti, sızma testine başlamadan önce plan yapılmasını sağlar
* ⚙️ WAF aktifse test araçlarının davranışı değiştirilebilir
* 🧠 Farklı payload ve bypass teknikleri kullanılabilir (örnek: WAF’li siteye XSS testini base64 ile yapmak)

**🎯 10. Öğrenim Kazanımları**

* Web uygulaması önünde WAF olup olmadığını tespit etmeyi öğrenme
* WAF sistemlerinin nasıl çalıştığını kavrama
* WAF bypass öncesi keşif aşamasında bilgi toplama pratiği
* HTTP istek/yanıt analizine dair farkındalık kazanma