**🧠 1. Graphw00f Nedir?**

**graphw00f**, bir hedef sitedeki **GraphQL endpoint’ine karşı kullanılan güvenlik duvarını (WAF/FW)** tespit etmeye yarayan bir **fingerprinting aracıdır.**

Amaç: Web uygulamasında GraphQL varsa, onu koruyan sistemin türünü tespit etmek.

📌 GraphQL endpoint’lerini pasif olarak tarayarak hangi tür korumaların aktif olduğunu anlamaya çalışır.

**🧰 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🧠 WAF tespiti | GraphQL isteklerine verilen yanıtlara göre WAF türünü tahmin eder |
| 🧪 Fingerprint analizi | Yanıt zamanlaması, hata mesajları, status kodlarına göre analiz yapar |
| 🧩 Basit, hafif ve modüler | Python tabanlıdır; kolay kurulur ve genişletilebilir |
| 📡 Endpoint doğrulaması | Gerçekten GraphQL mi, yoksa başka API mi kontrol eder |

**⚙️ 3. Kurulum (Kali Linux)**

**✅ Bağımlılıklar:**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🚀 4. Kullanım Komutları**

**✅ Temel kullanım:**

graphw00f -u http://target.com/graphql

**✅ Daha fazla çıktı almak için:**

graphw00f -u http://target.com/graphql -v

**✅ Proxy üzerinden taramak:**

graphw00f -u http://target.com/graphql --proxy http://127.0.0.1:8080

**✅ JSON çıktısı almak:**

graphw00f -u http://target.com/graphql -o json

**📋 5. Örnek Terminal Çıktısı**

**metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**📌 6. Ne Zaman Kullanılır?**

* **Pentest veya bug bounty sırasında GraphQL endpoint bulunursa**
* **Hangi WAF/FW sisteminin koruma sağladığı öğrenilmek istenirse**
* **Hedef sistemin zafiyet taramasına geçmeden önce fingerprint analizi yapılmak istenirse**

**🎯 7. Öğrenim Kazanımları**

* **GraphQL endpoint nedir, nasıl test edilir**
* **Web güvenlik duvarları nasıl tespit edilir**
* **WAF fingerprinting yöntemleri nasıl çalışır**
* **Web zafiyet testlerine hazırlık sürecinde temel analiz becerisi**