# WhatWaf Aracı - Eğitim Materyali

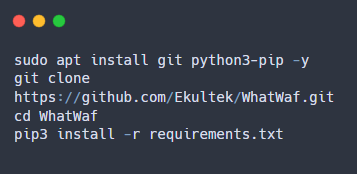
## 🧰 WhatWaf Nedir?

WhatWaf, bir web uygulamasının önünde bulunan güvenlik duvarı (WAF) çözümlerini tespit eden bir araçtır. Ayrıca bazı filtreleri atlamaya (bypass) çalışarak testler de yapabilir.  
  
- Python ile yazılmıştır  
- Açık kaynak kodludur  
- 100+ WAF imzası tanıyabilir  
- Basit komutlarla güçlü analizler yapar

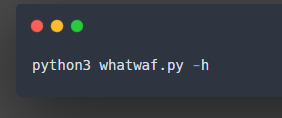
## 🛠️ Temel Özellikler

- 🔍 WAF Tespiti: Cloudflare, AWS WAF, ModSecurity gibi sistemleri tanır  
- 🧪 Bypass Testleri: WAF filtrelerinin tepkisini ölçer  
- 📂 Otomatik log: Taramaları kayıt altına alır  
- 🌍 Proksi desteği: Proxy üzerinden tarama yapılabilir

## 💻 Kali Linux Üzerinde Kurulum



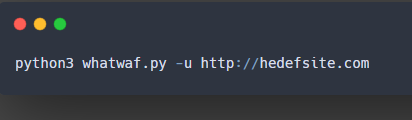
Çalıştırmak için:



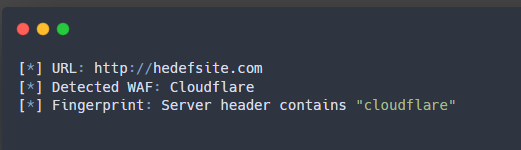
## 🧪 Kullanım Örnekleri

### ✅ Örnek 1: Temel WAF Tespiti

Komut:

******

Çıktı:



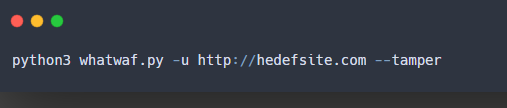
### ✅ Örnek 2: Proxy Üzerinden Tespit

Komut:

### 

### ✅ Örnek 3: Bypass Denemeleri ile Tespit

Komut:

******

Açıklama: WAF tarafından engellenebilecek istekler göndererek WAF'ın davranışı analiz edilir.

## ⚠️ Öğrenciler İçin Önemli Notlar (WhatWaf)

🔐 1. WAF, Güvenlik Duvarıdır — Gerçek Sitelerde Test Yapmayın:  
Sunucuya aşırı istek göndererek WAF sistemini devreye sokmak yasal sorunlar doğurabilir.  
  
🧪 2. “Tamper” Seçeneği Dikkatli Kullanılmalı:  
WhatWaf bazen agresif testler yapar, bu yüzden sadece test sistemlerinde kullanılmalıdır.  
  
📁 3. Loglar Önemlidir:  
Araç, tarama sonucunu .log dosyası olarak kayıt altına alabilir. Bunlar belgelemeye uygundur.