LFISuite - Eğitim Materyali

# 🧠 LFISuite Nedir?

LFISuite, web uygulamalarındaki Yerel Dosya Ekleme (LFI - Local File Inclusion) açıklarını tespit etmek ve bu açıklardan yararlanmak amacıyla kullanılan açık kaynaklı bir güvenlik aracıdır.  
LFI açıkları, saldırganların sunucu üzerindeki dosyalara erişmesine veya komut yürütmesine olanak tanır.

# 🚀 Özellikleri

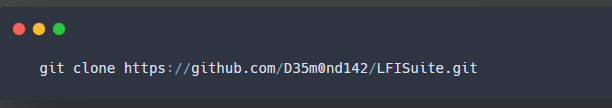
- Otomatik LFI açığı taraması  
- LFI yoluyla parola dosyası (e.g., /etc/passwd) okuma  
- Null byte (null karakter) testleri  
- Otomatik payload üretimi  
- Basit komut satırı arayüzü

# 🎯 Kullanım Alanları

- LFI güvenlik açığı taramaları  
- Zafiyetli web uygulamalarının test edilmesi  
- Eğitim ve CTF (Capture The Flag) ortamlarında sömürü senaryoları  
- Web uygulama güvenliği eğitimi

# 🛠️ Kurulum

1. GitHub üzerinden klonlayın:

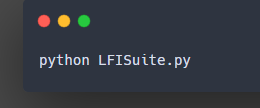
******

2. Dizine girin ve çalıştırın:

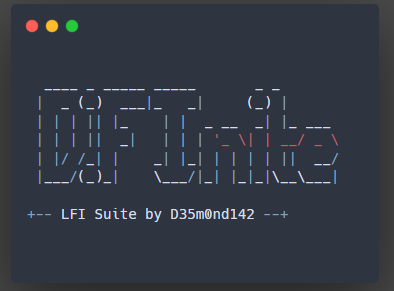
# 

# 🧪 Örnek Kullanım ve Terminal Çıktıları

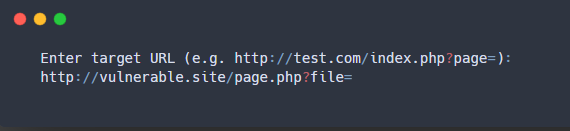
✅ 1. Uygulama çalıştırma:

******

Çıktı:

******

✅ 2. Hedef Belirtme ve Test Başlatma:

******

Çıktı (örn. /etc/passwd okuma):

# 

# 📎 Notlar

- Araç Python 2 için tasarlanmıştır, Python 3 ile uyumsuz olabilir.  
- Gelişmiş LFI teknikleri için manuel müdahale gerekebilir.  
- Eğitim ortamlarında etik kullanım amaçlı uygundur.  
- Hedef URL'de test edilecek parametrenin doğru seçilmesi gerekir (ör. page, file, path).