**Fimap Nedir?**

**Fimap**, dosya içerme (File Inclusion) zafiyetlerini tespit etmek ve bu açıklıkları istismar etmek için kullanılan açık kaynak kodlu bir siber güvenlik aracıdır. Python dili ile geliştirilmiş olan bu araç, özellikle **LFI (Local File Inclusion)** ve **RFI (Remote File Inclusion)** zafiyetlerinin otomatik olarak bulunması ve test edilmesi amacıyla kullanılır.

Web uygulamalarında sıkça rastlanan dosya içerme açıkları, saldırganlara sistem dosyalarına erişme, hassas bilgileri görüntüleme veya komut çalıştırma imkânı verir. Fimap, bu tür açıkların varlığını kontrol ederek güvenlik testlerinde önemli bir rol oynar.

**Dosya İçerme Zafiyetleri Nedir?**

* **LFI (Local File Inclusion):** Uygulamanın sunucudaki yerel dosyaları çağırmasına izin veren bir açıklıktır. Örneğin bir saldırgan, ../../etc/passwd gibi dizin dolaşma teknikleriyle sistem dosyalarına erişebilir.
* **RFI (Remote File Inclusion):** Uygulamanın dış bir kaynaktan (örneğin saldırganın kendi sunucusundan) dosya dahil etmesine olanak tanıyan açıklıktır. Bu açık, genellikle uzaktan zararlı PHP kodları çalıştırmak için kullanılır.

Fimap, bu iki tür açığı hem tespit eder hem de istismar edebilir.

**Fimap’in Temel Özellikleri**

* **LFI ve RFI tespiti:** URL'lerde parametreleri analiz ederek içerme açıklığı olup olmadığını kontrol eder.
* **Otomatik tarama:** Birden çok URL'yi aynı anda test edebilir.
* **Dosya sistemine erişim:** LFI açığını kullanarak passwd, shadow, log, config.php gibi kritik dosyaları çekebilir.
* **Komut çalıştırma (RCE):** Açıklık uygunsa, dosya içerme yoluyla uzaktan komut çalıştırılabilir.
* **Exploit desteği:** Bazı RFI açıklıkları üzerinden ters bağlantı (reverse shell) kurabilir.
* **Zayıf log dosyası keşfi:** Apache, Nginx gibi web sunucularında log injection ile exploit gerçekleştirebilir.
* **Kolay yapılandırma:** Basit komut satırı arayüzü ile çalışır; Python script olarak hızlıca başlatılabilir.

**Kurulum**

Fimap, Python 2 ile uyumludur. Python 2’nin kurulu olduğu sistemlerde aşağıdaki adımlarla kurulabilir:

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

⚠️ Python 2’nin artık resmi desteği sona erdiğinden, yeni sistemlerde çalıştırmak için güncelleme veya sanal ortam gerekebilir.

**Avantajları ve Dezavantajları**

**Avantajları:**

* Açık kaynak ve ücretsizdir.
* Otomatik tarama yeteneğiyle hızlı test yapılabilir.
* Komut satırı tabanlı olduğu için script otomasyonuna uygundur.
* LFI/RFI gibi zor tespit edilen açıklıkları başarıyla analiz eder.

**Dezavantajları:**

* Python 2 tabanlı olması nedeniyle güncel sistemlerde sorun çıkarabilir.
* Geliştirme desteği sınırlıdır, bazı özellikleri güncel web uygulamalarında çalışmayabilir.
* GUI desteği yoktur, sadece CLI ile çalışır.

**Etik ve Güvenlik Uyarısı**

Fimap gibi araçlar yalnızca eğitim, araştırma ve yetkili güvenlik testleri amacıyla kullanılmalıdır. Türkiye’de ve dünyanın birçok yerinde izinsiz güvenlik testi yapmak yasaktır ve cezai sonuçları vardır.

**Yalnızca şunlara karşı test yapmalısın:**

* Kendi web uygulamaların,
* Açık olarak izin verilmiş hedefler (örneğin bug bounty programları),
* Yasal olarak yetkilendirildiğin sistemler.

Aksi takdirde bu tür araçların kullanımı **siber suç** kapsamında değerlendirilir.

**Çalışır vaziyetteki bir örneğe göz atalım:**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.