LFI (Local File Inclusion) Eğitim Materyali

# 1. LFI Nedir?

LFI (Local File Inclusion), yani Yerel Dosya Dahil Etme, bir web uygulamasının sunucudaki dosyaları yetkisiz bir şekilde okumaya çalıştığı bir güvenlik açığıdır.  
Örneğin, kullanıcıdan alınan bir dosya adı doğrudan sistemdeki dosyalarla birleştirilirse, kötü niyetli biri hassas dosyaları görebilir.

# 2. LFI Nasıl Oluşur?

LFI genellikle aşağıdaki gibi bir URL'de ortaya çıkar:  
  
  
Eğer bu sayfa, kullanıcının verdiği 'page' değerini filtrelemeden doğrudan dosya olarak dahil ederse:  
include($\_GET['page']);  
  
O zaman şu şekilde suistimal edilebilir:  

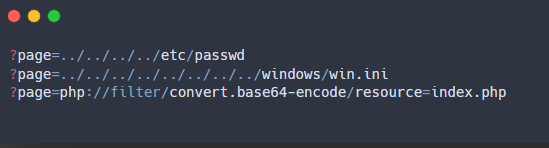

# 3. LFI ile Neler Yapılabilir?

- Sistem bilgilerini görüntüleme  
- Kullanıcı adı ve şifre dosyalarına erişme  
- Uzaktan komut çalıştırma (bazı senaryolarda)  
- Web sunucusunun dosya yapısını keşfetme

# 4. Örnek Senaryo

  
Saldırgan bunu şu şekilde değiştirirse:  
  
Eğer sunucu Windows ise bu sistem dosyasını ekranda gösterebilir.

# 5. LFI Tespiti (Manuel Test)

Test girdileri:  


# 6. Eğitim İpuçları

- Dosya yollarını anlatmak: ../ ne işe yarar?  
- Gerçek hayattan örneklerle öğretin (örneğin: klasör içindeki bir dosyayı açmak gibi).  
- Öğrenciler kendi PHP dosyalarında LFI oluşturup çözümleyebilirler.  
- include() fonksiyonu ve güvenlik kontrolleri üzerinde durulmalı.

# 7. Korunma Yöntemleri

- Dosya adı girişi kesinlikle filtrelenmeli  
- Sabit dosya listeleri (beyaz liste) kullanılmalı  
- realpath(), basename() gibi fonksiyonlarla yol manipülasyonu engellenmeli  
- allow\_url\_include ve display\_errors gibi ayarlar kapatılmalı

# 8. Etik Uyarı

LFI açıklarını test etmek güçlü bir yetkidir.  
Sadece kendi geliştirdiğiniz uygulamalarda ya da izinli sistemlerde denemeler yapılmalıdır.  
İzinsiz taramalar etik dışı ve yasa dışıdır.

# 9. LFI Test Ortamı Kurulumu ve Öğretimi

Öğrenciler için bir test ortamı kurmak için DVWA, Mutillidae veya kendi PHP dosyalarını kullanabilirler.  
Basit bir include($\_GET['page']); örneğiyle açık gösterilir.

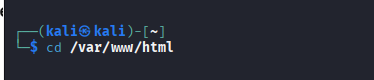
Ardından white-listing yöntemiyle nasıl kapatıldığı gösterilir.

✅ **Adım Adım: Kali Linux Üzerinde LFI Açığını Test Et**

**🚀 Plan: Kendi Basit LFI Sayfamızı Yazalım**

Kolayca ve güvenlik problem yaşamamak için kendi açığımızı kendimiz oluşturup test edeceğiz.

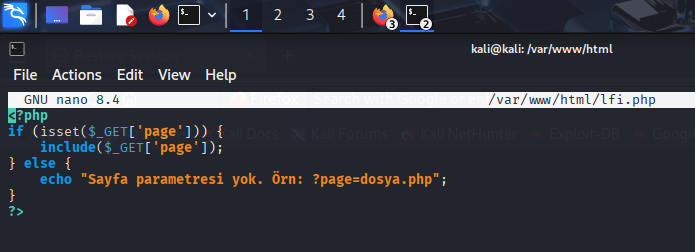
🔹 1. Apache dizinine geç



🔹 2. Dosya oluştur



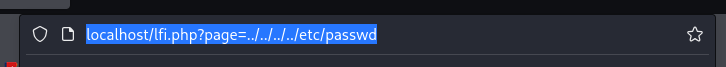
🔹 3. Zafiyet içeren kodu yazalım:



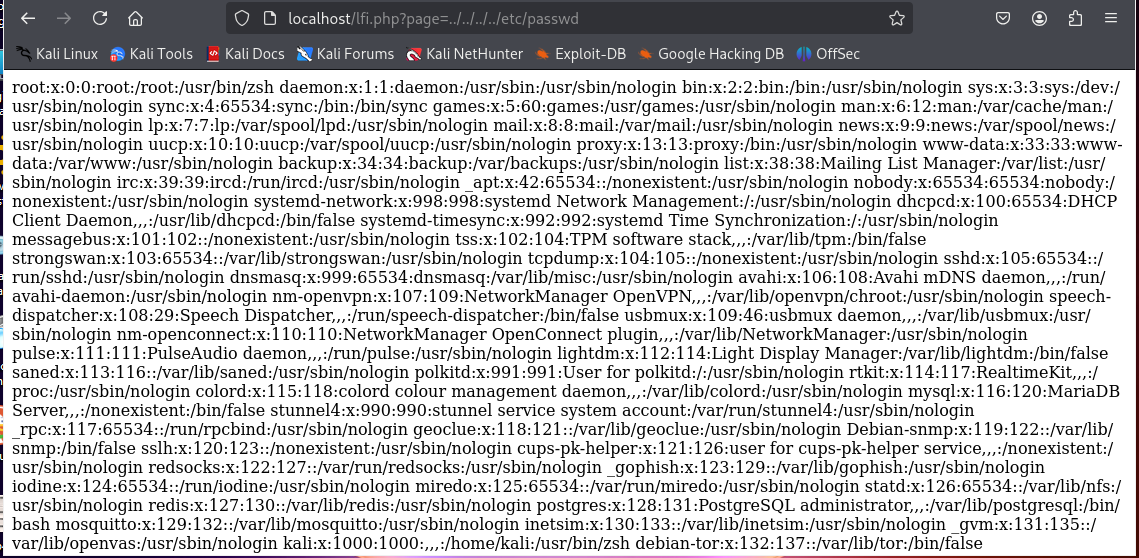
Kaydet → Ctrl+O → Enter → Çık → Ctrl+X

🔹 4. Test Et

Tarayıcıya şunu yaz:



Çıktı:



Bu şekilde olursa dosyaya erişebildik demektir. Peki nasıl yorumlayacağız?

Örneğin:

root:x:0:0:root:/root:/usr/bin/zsh

* root — Kullanıcı adı
* x — Şifre alanı, x görünmesi şifrelerin /etc/shadow dosyasında saklandığını gösterir
* 0 — Kullanıcı ID (UID), root kullanıcısı genellikle 0’dır
* 0 — Grup ID (GID)
* root — Kullanıcı tanımı veya açıklaması
* /root — Kullanıcının ana dizini
* /usr/bin/zsh — Kullanıcının girişte kullanacağı kabuk (shell), burada Z shell (zsh) kullanılıyor

Yani, bu dosya **sistemdeki kullanıcı hesaplarının ve onların temel bilgilerin kayıtlı olduğu yerdir.**