WEB GUVENLIGI TARAMASİ VE LFI ANALIZI

Web Güvenliği Taraması ve LFI (Yerel Dosya Dahil Etme) Analizi

-Projenin Amacı Ne? Bu projede, basit bir web uygulamasında ufak güvenlik testleri yapmak ve LFI (Local File Inclusion) denilen açığı araştırdık. Bu analizi yapmamızdaki amaç, siber güvenlik hakkında biraz fikir edinmek ve özgeçmişimize ekleyebileceğimiz bir proje oluşturmaktı.
Hangi Araçları Kullandık?Şu araçları kullandık:

- Nmap
- WhatWeb
- Nikto
- Burp Suite (Ücretsiz sürüm)
- Firefox/Chrome Tarayıcı

1. Senaryo ve Hedef Sistem (Kurban Sistem)Hedef sistem olarak TryHackMe veya benzeri bir test ortamındaki basit, zafiyetli bir web uygulamasını kullandık. Bu web sunucusuna internet üzerinden (HTTP) erişilebiliyor ve içinde LFI gibi açıklar barındırıyor olabilir.

- Güvenlik Analizi Adımları
Nmap ile Port Taraması YaptıkKomut:
nmap -sC -sV 10.10.10.10

- Sonuç: 80/tcp açık (Apache httpd), 22/tcp açık (SSH) çıktı.

-WhatWeb ile Teknolojiye BaktıkKomut:
whatweb http://10.10.10.10

- Sonuç: Apache 2.4.29, PHP 7.2.24 ve Ubuntu Server kullandığı anlaşıldı.
- Nikto ile Güvenlik Taraması YaptıkKomut:
nikto -h http://10.10.10.10
- Sonuç:
/admin dizini bulunabilir, X-Frame-Options eksik ve dizin listeleme açık olabilir gibi sonuçlar verdi.

- LFI Açığını Test Ettik.
- Şöyle bir zayıf URL parametresi test ettik:
http://10.10.10.10/index.php?page=../../../../etc/passwd
- Sonuç: Sunucu, dosya içeriğini hiçbir filtreleme yapmadan gösterdi. İşte bu, LFI açığı demek!
- Burp Suite ile Girdileri Analiz EttikBurp Suite ile URL parametrelerini ve form girişlerini inceledik. Girdi kontrolü yapılmadığını gördük.
- Sonuç ve ÖnerilerBu çalışmayla, basit web tarama araçları kullanarak LFI gibi önemli bir açığı bulduk. Bu tür açıklardan korunmak için kullanıcıların girdiği bilgiler mutlaka filtrelenmeli ve güvenli kodlama teknikleri kullanılmalı.

Rapor tarihi	08/07/2025