[Énumération/Web] LFI - RFI

Introduction

Les vulnérabilités **LFI** pour *Local File Inclusion* et **RFI** pour *Remote File Inclusion* sont très dangereuses puisqu'elles peuvent aboutir à des RCE dans certains cas ou l'affichage de fichiers systèmes comme /etc/shadow et /etc/passwd .

Ces failles reposent sur la possibilité pour l'utilisateur d'un site web de pouvoir appeler un fichier dont il ne doit pas avoir accès initialement.

Là où la LFI se contente de pouvoir appeler des fichiers locaux au serveur web, la RFI permet d'ouvrir un fichier distant.



LFI Finder Tool

Un outil très pratique qui permet d'énumérer les LFI disponibles d'une application web :

https://github.com/capture0x/LFI-FINDER

Revision #4
Created 2023-10-26 09:09:39 UTC by Elieroc
Updated 2024-05-03 14:36:16 UTC by Elieroc