# Pentest en utilisant DVWA

>author : Sacha Besser

# 1. Local File Inclusion

Une **Local File Inclusion (LFI)** est une vulnérabilité web qui permet à un attaquant de forcer un site à inclure et afficher des fichiers locaux présents sur le serveur.

Cette faille se produit lorsque le site web inclut un fichier sans bien vérifier ou filtrer ce que l’utilisateur peut choisir.

Par exemple, un site utilise une URL comme :

```

<http://34.163.97.167/DVWA/vulnerabilities/fi/?page=file.php>

```

Ici, le fichier file.php est inclus par la variable page.

Si l’entrée utilisateur n'est pas sécurisée, un attaquant pourrait manipuler l'URL pour inclure d'autres fichiers locaux :

```

<http://34.163.97.167/DVWA/vulnerabilities/fi/?page=>/etc/passwd

```

## 1.1 Premier niveau – low

Nous avons une page toute simple avec trois fichiers` <http://34.163.97.167/DVWA/vulnerabilities/fi/?page=include.php> `

![image](images/lfi/1.png)

Nous allons donc simplement essayer de modifier le parametre pour inclure une autre page par exemple `/etc/passwd`

```

<http://34.163.97.167/DVWA/vulnerabilities/fi/?page=>../../../../etc/passwd

```

![image](images/lfi/2.png)

On voit que la faille est bien présente puisqu’elle permet d’afficher n’importe quel fichier sur le serveur.

On peut donc en quelque sorte en déduire le code php qui est présent sur le serveur.

```

<?php

$page = $\_GET['page'];

include($page); ?>

```

Cela serait probablement quelque chose comme affiche ci-dessus. C’est-à-dire un simple paramètre `GET` sans aucune structure de contrôle.