local file inclusion

-lfi definition:

The File Inclusion vulnerability allows an attacker to include a file, usually exploiting a dynamic file inclusion mechanisms implemented in the target application. The vulnerability occurs due to the use of user-supplied input without proper validation.

it also known as that is the process of including files, that are already locally present on the server, through the exploiting of vulnerable inclusion procedures implemented in the application.

Function that could result in lfi:

1-include ()

2-inculde _once()

3-require ()

4-require_once()

local file disclosure : the same as local file inclusion but it enable be te execute file not only read it .

note : every lfi can be lfd but every lfd not nessery to be lfi

remote file inclusion: A remote file inclusion (RFI) occurs when a file from a remote web server is inserted into a web page. This can be done on purpose to display content from a remote web application. But, it can also happen by accident, due to a misconfiguration of the respective programming language, wchich can lead to a RFI attack.

Even though this kind of file inclusion can occur in almost every kind of web application, those written in PHP code are more likely to to be vulnerable to Remote File Inclusion attacks, because PHP provides native functions that allow the inclusion of remote files. Other languages usually require a workaround to imitate this behavior.

How Does Remote File Inclusion work?

In order to include a remote file you have to add a string with the url of the file to an Include function of the respective language (for example, PHP). Then the web server of the website under attack makes a request to the remote file, fetches its contents and includes it on the web page serving the content. It is then processed by the parser of the language.

A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. It should be noted that access to files is limited by system operational access control (such as in the case of locked or in-use files on the Microsoft Windows operating system).

This attack is also known as “dot-dot-slash”, “directory traversal”, “directory climbing” and “backtracking”.