What is Local File Inclusion?

Local File Inclusion (LFI) is a web vulnerability where an application includes a file whose path the user controls, so an attacker reads files they should not, source code, configuration, `/etc/passwd`, and sometimes runs their own code. It happens when user input reaches a file-include call (such as PHP `include`) without validation. LFI often escalates to remote code execution through log poisoning, PHP wrappers, or session files, which is why it ranks among the most serious input-handling flaws.

HOW IT WORKS

01 How it works and example

The attacker manipulates the file parameter to read or run files:

- Read a sensitive file: `?page=../../../../etc/passwd`
- Read source via a PHP filter wrapper: `?page=php://filter/convert.base64-encode/resource=config.php`
- Escalate to code execution by log poisoning: inject PHP into a User-Agent header that gets logged, then include the log file (`/var/log/apache2/access.log`).
- Include an uploaded file or a session file containing attacker input.

Remote File Inclusion (RFI), the related flaw, includes a file from a remote URL when the configuration allows it, giving direct code execution. Examples shown for defensive context.

> LFI TO RCE
>
> *LFI is dangerous because it rarely stops at reading files. Log poisoning, PHP wrappers, and session inclusion routinely turn an LFI into remote code execution, so treat any LFI as critical.*

HOW TO DEFEND

- Never build include paths from user input. Map user choices to a fixed allow-list of files server-side, never to a raw path.
- Disable remote includes (`allow_url_include=Off` in PHP) to kill RFI.
- Validate and canonicalise any unavoidable path input and reject traversal sequences after normalisation.
- Run with least privilege so an included file cannot reach sensitive locations.
- Confirm with a penetration test that no parameter reaches a file-include sink.

SOURCES

[1] OWASP Web Security Testing Guide

[2] MITRE CWE-98: Improper Control of Filename for Include/Require

[3] OWASP Top 10

Test your application for LFI and 30+ other classes.

`securelayer7.net/learn/application-security/local-file-inclusion`

Open online