

---

## ***LFI & LFD & LFR***

---

### 1. **LFI** (Local File Inclusion)

- LFI happens when a web application **includes** (loads) a local file from the **same server** insecurely, usually due to improper input validation.
- **Goal:** Read or execute local files (from the target's file system).
- **Impact:**
  - Reading sensitive files.
  - Sometimes leading to code execution (if log files or session files are included).

### 2. **LFD** (Local File Disclosure)

- LFD is a **result or consequence** of LFI.
- It specifically refers to the **ability to read or disclose** files from the local system, **without necessarily executing them**.
- **Goal:** Extract local files, **No code execution**, just reading.
- 

### 3. **LFR** (Local File Read)

- This is basically another name for **LFD** — they are often used interchangeably.
- LFR emphasizes that the attacker can **read** local files but not necessarily execute them.
- **Goal:** Read local files

**In short:** **LFD** and **LFR** are basically the same class of impact. They let an attacker **read files on the target system**. That read-only ability can still produce very high impact.

#### **Some Impacts:**

- **Credentials & secrets**
- **Source code**
- **Configurations**
- **Personal data**
- **Internal endpoints**
- **Session tokens / cookies**
- **Logs**

## **SOP (Standard Operating Procedures)**

Standard operating procedures (SOPs) are processes that **include a set of written instructions** that help security practitioners follow a straightforward and well-laid-out framework to achieve optimum efficiency in task completion. The goal of **SOPs** is to allow analysts to **find the most efficient path** to completing complex and repetitive tasks by following step-by-step guidelines.

**In short:** It's the rulebook or manual for how cybersecurity operations should be done safely and correctly.

**Purpose:** SOPs make sure everyone in the security or IT team:

- Follows the same secure process.
- Responds to incidents quickly and correctly.
- Reduces human error and insider threats.