**5️⃣ Testing for Local File Inclusion (LFI)**

**🔹 What is it?**

* Attacker includes **local server files** via parameters.

**🔹 Example**

include($\_GET['page']);

Payload:

?page=../../../../etc/passwd

**🔹 Testing**

* **Manual**: Try ../ traversal payloads.
* **Burp Suite/ZAP**: Fuzz page= with wordlists (/etc/passwd, C:\boot.ini).
* **Indicators**: File contents in response.

**🔹 Mitigation**

* Whitelist allowed files.
* Use framework’s secure file loaders.