**7️⃣ Testing for OS Command Injection**

**🔹 What is it?**

* User input executed as **system commands**.

**🔹 Example**

system("ping " . $\_GET['ip']);

Payload:

127.0.0.1; cat /etc/passwd

**🔹 Testing Methods**

* **Manual**: Append ; id, && whoami.
* **Burp Suite**: Intercept → inject payloads → observe response.
* **ZAP Proxy**: Use Active Scan rules.
* **Commix Tool**: Automates command injection testing/exploitation.

**🔹 Indicators**

* Extra output (user, system info).

**🔹 Mitigation**

* Use safe APIs (execve with args, not concatenated strings).
* Input whitelisting.