**8️⃣ Testing for Format String Injection**

**🔹 What is it?**

* Occurs when user input is passed directly to **printf-style functions**.

**🔹 Example**

printf(userInput);

Payload:

%s%s%s%s

**🔹 Impact**

* Memory disclosure, crashes, possibly RCE.

**🔹 Testing**

* Inject %x, %s, %n → see if system leaks memory.

**🔹 Mitigation**

* Never pass user input directly as format strings.