**2️⃣ Testing for XPath Injection**

**🔹 What is it?**

* Manipulating input used in an XPath query to bypass authentication or extract XML data.

**🔹 Example Vulnerable Code**

String query = "//user[username/text()='" + user + "' and password/text()='" + pass + "']";

Payload:

' or '1'='1

**🔹 Testing Steps**

* **Manual**: Inject ' or '1'='1 or '] | //user/\*[username='admin'] | ['a'='a into fields.
* **Burp Suite**: Send login requests → inject XPath payloads → check different server responses.
* **Indicators**: Different error messages like XPath syntax error.

**🔹 Mitigation**

* Use **parameterized XPath queries**.
* Strong input validation.