**3️⃣ Testing for IMAP/SMTP Injection**

**🔹 What is it?**

* Some apps interact with **mail servers** (IMAP/SMTP) using user-controlled input.
* If input is concatenated directly into IMAP/SMTP commands, attacker can inject commands.

**🔹 Example**

$mail = "{mail.example.com:143/imap}INBOX";

$mbox = imap\_open($mail, $username, $password);

Payload for username:

testuser) UID SEARCH ALL

**🔹 Impact**

* Attacker can read arbitrary emails, bypass authentication, or send unauthorized mail.

**🔹 Testing**

* **Manual**: Try payloads like test\r\nRCPT TO:<attacker@example.com> in email fields.
* **Burp Suite**: Intercept email-related requests, fuzz with \r\n and SMTP commands.

**🔹 Mitigation**

* Strictly sanitize email-related input.
* Use secure APIs instead of raw IMAP/SMTP command concatenation.