Got it ✅ You’re studying **WSTG (Web Security Testing Guide)**. Let’s make precise, beginner-friendly notes for **Testing for HTTP Incoming Requests (WSTG-CLNT-09 in v4.2)**.

**📝 Notes: Testing for HTTP Incoming Requests**

**🎯 Purpose**

To check whether a web application **processes unexpected HTTP requests sent to the client** (browser, mobile app, or thick client).  
Some applications may **open a local service/port** to receive incoming requests. If not properly secured, attackers can exploit it.

**⚡ Common Scenarios**

1. **Localhost Binding**
   * Application runs a service (e.g., on http://127.0.0.1:xxxx).
   * Attackers can send requests to it via CSRF, SSRF, or malicious sites.
2. **Custom Protocols**
   * Apps may register a custom protocol handler (e.g., myapp://).
   * If insecure, attackers can trigger unwanted actions.
3. **Cross-protocol Requests**
   * Sending unexpected HTTP traffic to services that don’t expect it (e.g., databases, message queues).

**🔍 How to Test**

1. **Identify Local Services**
   * Run the app and check if it opens ports on localhost.
   * Tools: netstat, lsof, nmap.
2. **Send Malicious Requests**
   * Try to craft HTTP requests targeting the local service.
   * Example: force the browser to make a request via <img src="http://127.0.0.1:xxxx/sensitive-endpoint">.
3. **Check for CSRF-like Behavior**
   * If requests are executed without authentication → **vulnerable**.
4. **Protocol Abuse**
   * Attempt sending crafted requests via custom protocol schemes.

**🛡️ Mitigation**

* Do **not expose local HTTP listeners** unless strictly necessary.
* Require **authentication & tokens** for any local request.
* Implement **CORS restrictions** and **same-origin policy enforcement**.
* Validate **protocol handlers** and avoid unsafe URL schemes.

✅ **Key Takeaway:**  
This test ensures the app does not unintentionally accept or process HTTP requests locally (browser or client). Such issues can allow CSRF, SSRF, or privilege escalation.

Do you want me to also prepare **step-by-step practical testing commands/examples** (like nmap, BurpSuite payloads, etc.) for this, or just keep it as conceptual study notes?