Great — let’s make **precise WSTG-style notes** for **Introduction to Business Logic Testing** 👇

**📝 Notes: Introduction to Business Logic**

**🎯 Purpose**

Business Logic Testing focuses on identifying **flaws in how the application is designed to handle workflows, rules, and processes**, rather than purely technical vulnerabilities.

These flaws often cannot be detected by automated scanners — they require **manual testing & understanding of the application’s intended behavior**.

**⚡ Examples of Business Logic Issues**

1. **Bypassing workflow steps**
   * e.g., Skipping payment step and directly accessing the "Order Confirmation" page.
2. **Manipulating Parameters**
   * e.g., Changing product price from 100 → 1 in hidden fields.
3. **Excessive Actions**
   * e.g., Unlimited password reset attempts → account takeover.
4. **Privilege Escalation**
   * e.g., Normal user accessing admin-only functions by modifying requests.
5. **Concurrency Issues**
   * e.g., Placing multiple orders by abusing race conditions.

**🔍 How to Test**

1. **Understand the Application Flow**
   * Map workflows (e.g., registration, checkout, transfer of funds).
   * Identify intended rules & constraints.
2. **Look for Trust Assumptions**
   * Does the app trust user input too much?
   * Are critical checks happening only on client-side?
3. **Attempt Logical Abuse**
   * Bypass steps, change sequence, replay requests, or manipulate hidden parameters.
4. **Test Negative Scenarios**
   * Input invalid data, skip steps, submit duplicate requests.

**🛡️ Mitigation**

* Enforce **server-side validation** of business rules.
* Use **state validation** (ensure users cannot skip steps).
* Apply **rate limiting & anti-automation controls**.
* Conduct **threat modeling** during design to anticipate abuse cases.
* Regularly review workflows for **logic gaps**.

✅ **Key Takeaway:**

Business logic flaws = **design mistakes** in workflows.

They usually won’t show up in vulnerability scans → only detected through **manual, context-aware testing**.

Do you want me to also make a **step-by-step checklist** (like a tester’s playbook) for business logic testing workflows?