Nice — let’s lock down **WSTG notes for “Test Integrity Checks” (WSTG-BUSL-04)** 👇

**📝 Notes: Test Integrity Checks**

**🎯 Purpose**

To verify whether the application ensures the **integrity of critical data and workflow steps**.  
If integrity checks are missing, attackers can **tamper with parameters, tokens, or files** and trick the application into accepting maliciously altered data.

**⚡ Common Attack Scenarios**

1. **Parameter Tampering**
   * Changing price=100 → price=1 in hidden fields.
   * Editing loyalty points or discount codes.
2. **Replay / Reuse of Tokens**
   * Reusing old session tokens, reset links, or transaction IDs.
3. **Digital Asset Manipulation**
   * Modifying client-side stored files (e.g., config.json, cookies) to unlock premium features.
4. **Workflow Integrity**
   * Skipping mandatory steps (payment → confirmation) and still getting success response.

**🔍 How to Test**

1. **Identify Sensitive Data**
   * Parameters affecting price, role, balance, privileges, state transitions.
2. **Intercept & Modify Requests**
   * Use Burp Suite/ZAP/Postman.
   * Change hidden fields, cookies, or query params.
3. **Replay & Reuse**
   * Attempt reusing tokens (password reset, transaction links).
   * Submit duplicate/expired requests.
4. **Tamper with Client-Side Data**
   * Modify cookies, localStorage, or mobile app config files.
5. **Check Server-Side Controls**
   * Does the server verify the correctness of data? Or does it trust client blindly?

**🛡️ Mitigation**

* Validate **all critical data server-side** (never trust client-side values).
* Use **HMACs or digital signatures** to protect parameters/tokens.
* Implement **one-time-use tokens** for sensitive actions.
* Enforce **workflow state validation** (payment required before confirmation).
* Secure **cookies/local storage** with integrity protection (HttpOnly, Secure, signed values).

✅ **Key Takeaway:**  
Without strong **integrity checks**, attackers can manipulate business-critical data or reuse tokens → leading to fraud, privilege escalation, or bypass of payments.

👉 Do you want me to also create a **list of practical test payloads** (like examples for tampering price, replaying tokens, altering cookies) so you can use them directly in hands-on testing?