Alright 👍 let’s refine and give you **precise WSTG notes** for

**📝 Test Number of Times a Function Can Be Used Limits (WSTG-BUSL-06)**

**🎯 Purpose**

To ensure the application **enforces restrictions on how often a function can be executed**.  
If limits are missing, attackers may **abuse critical functions repeatedly** (e.g., brute force, multiple discounts, repeated withdrawals).

**⚡ Common Attack Scenarios**

* **Login attempts** → no lockout → brute-force possible.
* **Password reset** → unlimited reset requests → DoS on victim.
* **Promo codes/coupons** → reused many times → financial fraud.
* **Transaction limits** → split large transfer into many smaller ones.
* **Resource-heavy APIs** → unlimited calls → DoS or scraping.

**🔍 How to Test**

1. **Identify Limited Functions**
   * Authentication, password reset, voucher redemption, payments, file downloads, API endpoints.
2. **Exceed the Expected Limit**
   * Try >3–5 failed logins.
   * Reuse the same coupon repeatedly.
   * Submit excessive password reset requests.
3. **Automation / Tools**
   * **Burp Intruder** / **OWASP ZAP** → send many requests.
   * **curl loop** for quick tests:
   * for i in {1..20}; do
   * curl -X POST https://target.com/login -d "user=a&pass=wrong";
   * done
4. **Check for Weak Rate Limiting**
   * Rotate IPs (X-Forwarded-For, VPN).
   * Use multiple accounts.
   * Send requests in parallel (race condition).

**🛡️ Mitigation**

* Enforce **server-side counters** (per account, per IP, per device).
* Apply **rate limiting / throttling** (e.g., max 5 attempts per minute).
* Use **CAPTCHA** after repeated attempts.
* Invalidate vouchers after single use.
* Implement **atomic operations** → one transaction = one execution.
* Monitor & alert on abnormal usage patterns.

✅ **Key Takeaway:**  
Without strict **usage limits**, attackers can **brute-force, abuse vouchers, bypass transaction rules, or DoS the system**.

👉 Do you want me to now create a **ready-to-use tester’s checklist** (like: try 5+ logins, resend reset tokens, redeem coupon N times, etc.) so you can directly apply during assessments?