Perfect — **Testing for Default Credentials** is another classic **WSTG authentication weakness check** 🔎.

**🧾 Testing for Default Credentials**

**1. Why It Matters**

* Many applications, routers, databases, and admin panels ship with **default usernames/passwords** (like admin/admin, root/toor, guest/guest).
* If administrators forget to change them → attackers can log in easily.
* Real-world breaches often start from forgotten dev/test systems with defaults enabled.

**2. What to Test**

🔹 **Web Apps / Admin Panels**

* /admin, /login, /phpmyadmin, /manager/html (Tomcat), etc.

🔹 **Databases & Services**

* MySQL → root / (blank)
* MongoDB → no password (older versions)
* Postgres → postgres/postgres

🔹 **Network Devices**

* Cisco → cisco/cisco
* D-Link, Netgear, TP-Link often ship with admin/admin

🔹 **Applications / Frameworks**

* Jenkins, Wordpress, Drupal, Tomcat, etc.

**3. Tools & Techniques**

**🔸 Manual Testing**

* Try **known vendor defaults** (check vendor docs, community lists).

**🔸 Hydra / Medusa / Ncrack**

Automated brute-force tools with username/password lists.

hydra -L users.txt -P passwords.txt http-get://example.com/login

**🔸 Nmap NSE (default-creds script)**

nmap --script vuln,default -p 22,23,80,443 <target>

* The default script attempts known default creds for services.

**🔸 Search in Exploit Databases**

* Default creds lists → [SecLists](https://github.com/danielmiessler/SecLists) (/Passwords/Default-Credentials/).

**4. Indicators of Default Credentials**

* Successful login with **simple/common pairs**.
* Admin dashboards exposed without MFA.
* Database access without authentication.

**5. Preventive Controls**

✅ Always **change defaults immediately** after install.  
✅ Enforce **unique strong passwords** per service.  
✅ Deploy MFA for admin accounts.  
✅ Regularly audit with vulnerability scanners (Nessus, OpenVAS).  
✅ Disable or restrict unused accounts (e.g., guest).

✅ **Summary**:  
Testing for default credentials = attempt logins using **vendor-provided or common username/password pairs**. Tools like Hydra, Nmap NSE, and SecLists make this systematic.

👉 Do you want me to build you a **Challenge Lab scenario (e.g., Tomcat admin panel with default creds)** so you can practice this safely?