BUG BOUNTY CHECKLIST (TOOL-BASED)

0) BEFORE ANYTHING

- Read scope and rules

- Note allowed/out-of-scope domains

- Create 2 test accounts

1) SETUP

- Install Burp Suite, Postman, Browser extensions

- Configure proxy and logging

2) PASSIVE RECON

- subfinder -d target.com -all -o subs.txt

- httpx -l subs.txt -o alive.txt

3) AUTOMATED CHECKS

- nuclei -l alive.txt -t takeovers/ -t exposures/

4) MANUAL RECON (Burp)

- Map all pages, forms, parameters, file uploads

5) CONFIGURATION SECURITY

- HTTPS enforcement

- Cookie flags: Secure, HttpOnly, SameSite

- Security headers

6) AUTHENTICATION TESTING

- Login flow

- Password reset

- Session rotation

7) AUTHORIZATION (IDOR)

- Replace user IDs

- Test horizontal/vertical privilege escalation

8) INPUT TESTING

- XSS payload: ">alert(1)

- SQL/NoSQL error-based checks

9) CSRF

- Remove or modify CSRF token

10) FILE UPLOAD TESTS

- MIME checks

- Extension bypass

- Executability

11) SSRF & WEBOOKS

- Safe external URLs

12) API TESTING

- Remove Authorization header

- Excessive data exposure

13) BUSINESS LOGIC

- Skip steps

- Double-submit

- Coupon reuse

14) REPORTING

- Steps to reproduce

- Impact

- Evidence

15) FINAL CHECKLIST

- Recon

- Surface checks

- Auth

- AuthZ

- Input

- CSRF

- File upload

- API

- Logic