COMPLETE BUG BOUNTY CHECKLIST

-By Alham Rizvi

- **Your Name / Hunter Alias:**
- **Company / Organization Name:**
- **Program Name:**
- **Target Domain(s) / URL(s):**
- **Platform Name:** (HackerOne / Bugcrowd / Intigriti / Private)
- **Program Type:** (Public / Private / VDP)
- **Start Date:**
- **End Date (optional):**
- **Out of Scope:**

□ COMPLETE BUG BOUNTY CHECKLIST

1. Recon & Attack Surface Discovery

Passive Recon

☐ Read program rules & scope carefully
☐ Identify web apps, APIs, mobile apps
☐ Discover domains & subdomains
☐ Google dorking
☐ GitHub recon (secrets, endpoints)
☐ JavaScript file analysis
☐ API endpoint discovery
☐ Technology fingerprinting

Active Recon

☐ Directory & file discovery
☐ robots.txt & sitemap.xml
☐ Admin panels
☐ Backup & config files
☐ Screenshot mapping
☐ Open ports & services (if allowed)

2. LOW HANGING FRUITS (FAST WINS)

Authentication & Session

☐ No rate limiting
☐ Brute-force protection missing
☐ Weak password policy
☐ Password reset flaws
☐ Session fixation
☐ Session expiration issues

Access Control

☐ IDOR (horizontal)
☐ IDOR (vertical)

☐ Broken access control
☐ Forced browsing

Misconfigurations

☐ Missing security headers
☐ CORS misconfiguration
☐ Open redirect
☐ Debug endpoints
☐ Information disclosure

3. INPUT & CLIENT-SIDE VULNERABILITIES

XSS (All Types)

☐ Reflected XSS
☐ Stored XSS
☐ DOM-based XSS
☐ Blind XSS
☐ XSS via file upload
☐ XSS chaining

Client-Side Issues

☐ HTML Injection
☐ DOM manipulation
☐ Insecure postMessage
☐ Clickjacking

4. PARAMETER DISCOVERY & LOGIC

Parameter Issues

☐ Hidden parameters
☐ Unused parameters
☐ HTTP Parameter Pollution
☐ Mass assignment
☐ JSON parameter injection

Business Logic (Basic)

☐ Workflow bypass
☐ Step skipping
☐ Role confusion
☐ Validation inconsistencies

5. FILE & PATH VULNERABILITIES

File Issues

☐ Unrestricted file upload
☐ File type bypass
☐ File overwrite
☐ ZIP Slip

Path Issues

☐ Local File Inclusion (LFI)
☐ Remote File Inclusion (RFI)
☐ Path traversal
☐ Backup file exposure

6. INJECTION VULNERABILITIES

☐ SQL Injection – Error based
☐ SQL Injection – Boolean based
☐ SQL Injection – Time based
☐ Command Injection
☐ OS Injection
☐ SSTI
☐ Expression Language Injection

7. ADVANCED WEB ATTACKS (PORTSWIGGER CORE)

Server-Side Attacks

☐ SSRF
☐ Blind SSRF
☐ SSRF → Internal services
☐ SSRF → Cloud metadata
☐ HTTP Request Smuggling
☐ HTTP Desync
☐ Web Cache Poisoning
☐ Web Cache Deception

XML & Parsing

☐ XXE
☐ XPath Injection
☐ XML Injection

8. API & TOKEN VULNERABILITIES

API Security

☐ BOLA
☐ BFLA

☐ Excessive data exposure
☐ Mass assignment (API)
☐ Improper asset management
☐ Missing rate limits

Tokens & Auth

☐ JWT algorithm confusion
☐ Token reuse
☐ Token leakage

9. BUSINESS LOGIC & CHAINING

Advanced Logic

☐ Price manipulation
☐ Coupon abuse
☐ Payment bypass
☐ Refund abuse
☐ Race conditions
☐ Time-based logic flaws

Chaining

☐ XSS → Account takeover
☐ IDOR → Data exposure
☐ SSRF → Internal admin access
☐ Logic flaw → Financial impact

10. ADVANCED & EMERGING ATTACKS (OPTIONAL)

Platform-Specific

☐ WordPress vulnerabilities
☐ Plugin/theme issues
☐ XML-RPC abuse

Modern Attacks

☐ WebSockets vulnerabilities
☐ Prompt Injection (LLM attacks)
☐ Insecure AI integrations
☐ Third-party service abuse

11. REPORTING (NON-NEGOTIABLE)

☐ Clear reproduction steps
☐ Impact explained in business terms
☐ Proper severity rating

☐ Screenshots / PoC
☐ Retest after fix