🛡️ 30-Day Bug Bounty Checklist (Minimalist)

Name: ________________________
Start Date: ___________________
Daily Time: 1–2 hours

WEEK 1 — Web & Security Foundations

Day 1 — Web Basics
☐ HTTP vs HTTPS
☐ GET / POST
☐ Cookies & sessions
☐ Observe login request

Day 2 — Frontend vs Backend
☐ Frontend vs backend
☐ APIs
☐ Inspect forms
☐ Modify values

Day 3 — OWASP Basics
☐ OWASP Top 10
☐ What is a vulnerability
☐ Attacker mindset

Day 4 — XSS
☐ Reflected XSS
☐ Stored XSS
☐ Complete labs

Day 5 — Authentication
☐ Login flow
☐ Password reset
☐ Sessions

Day 6 — Authorization / IDOR
☐ Auth vs authorization
☐ Modify object IDs
☐ IDOR labs

Day 7 — Review
☐ Review week
☐ Repeat weak labs

WEEK 2 — Tools & Vulnerabilities

Day 8 — Burp Basics
☐ Proxy setup
☐ Intercept requests
☐ HTTP history

Day 9 — Repeater
☐ Send to Repeater
☐ Modify parameters

Day 10 — SQL Injection
☐ SQLi concepts
☐ Error-based SQLi

Day 11 — CSRF
☐ CSRF basics
☐ Tokens

Day 12 — File Upload
☐ Extension bypass
☐ MIME testing

Day 13 — Business Logic
☐ Workflow abuse

Day 14 — Recon Basics
☐ Endpoints
☐ JS / robots.txt

WEEK 3 — Real Bug Bounty Practice

Day 15 — Practice App
☐ Test without hints
☐ Find 1 bug

Day 16 — Read Reports
☐ Read 5 reports

Day 17 — Platforms
☐ HackerOne
☐ Bugcrowd

Day 18 — Pick Program
☐ Public
☐ Small scope

Day 19 — Manual Testing
☐ Auth flows
☐ Parameters

Day 20 — Deep Testing
☐ IDOR
☐ API

Day 21 — Validate
☐ Reproduce
☐ Impact
☐ In scope

WEEK 4 — Reporting & Growth

Day 22 — Write Report
☐ Summary
☐ Steps
☐ Impact

Day 23 — Re-test
☐ New account

Day 24 — Submit
☐ Submit report

Day 25 — Triage
☐ Read feedback

Day 26 — Learn
☐ Analyze result

Day 27 — Improve
☐ Practice weak area

Day 28 — Second Target
☐ Repeat testing

Day 29 — Chaining
☐ Low → high impact

Day 30 — Final Review
☐ Review month
☐ Set next goal

OTHER WAYS BUG BOUNTIES HAPPEN

API Security

☐ Missing auth
☐ Broken authorization
☐ Parameter tampering
☐ Rate-limit bypass

Mobile Apps

☐ Insecure APIs
☐ Hardcoded secrets
☐ Insecure storage

Infrastructure / Cloud

☐ Exposed services
☐ Misconfigured storage
☐ Debug endpoints

Desktop Apps

☐ Insecure updates
☐ Local privilege issues

Hardware / IoT

☐ Default credentials
☐ Insecure firmware

NOT Allowed

☐ Automated scanning
☐ Brute force
☐ DoS
☐ Out of scope

Beginner Focus

☐ Web apps
☐ APIs
☐ Manual testing
☐ Logic bugs