Vulnerability Discovery Readiness Checklist

Legal and Ethical Discipline

1. ☐ I only test inside authorized environments.
2. ☐ I understand responsible disclosure obligations.
3. ☐ I validate findings with minimal impact.

Reconnaissance and Mapping

4. ☐ I inventory endpoints before deep testing.
5. ☐ I inspect hidden requests and parameters.
6. ☐ I compare multiple account states.
7. ☐ I inspect archived or forgotten resources.

Authentication and Authorization

8. ☐ I test ownership validation carefully.
9. ☐ I inspect session handling and token reuse.
10. ☐ I compare user A versus user B access.

Input and Parameter Testing

11. ☐ I review all user-controlled fields as trust channels.
12. ☐ I change one variable at a time.
13. ☐ I inspect hidden fields and client-side values.

Configuration and Logic Review

14. ☐ I check for public file exposure and debug leaks.
15. ☐ I review workflow sequence assumptions.
16. ☐ I inspect business process bypass opportunities.

Workflow Discipline

17. ☐ I keep organised endpoint and hypothesis notes.
18. ☐ I capture screenshots and requests in real time.
19. ☐ I preserve reproducible evidence.

Reporting Maturity

20. ☐ I can write clear reproduction steps.

21. ☐ I explain impact calmly and accurately.
22. ☐ I include concise comparative proof.

Long-Term Research Growth

23. ☐ I focus on observation over hype.
24. ☐ I revisit targets deeply instead of moving too fast.
25. ☐ I treat vulnerability discovery as a professional discipline.

SCORING RESULTS

Strong Research Discipline (20–25 Checked)

You are building professional-grade vulnerability observation habits and ethical research maturity.

Developing Vulnerability Awareness (12–19 Checked)

You have meaningful exposure but need stronger consistency and structured methodology.

Early Discovery Stage (0–11 Checked)

You are still approaching testing too casually and should focus more on mapping, notes, and disciplined trust analysis.