MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

CAREER ROADMAP · 2026 EDITION

Bug Bounty to Red Team Professional Roadmap 2026

Build disciplined web research skills, high-quality reporting, and the broader capabilities needed for authorized red-team work.

5	6	100%
Progression stages	Portfolio assets	Authorized practice

mnatech.in @mna_tech_academy +91 9216110094

MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

How to use this guide

Treat this roadmap as a competency plan, not a promise of salary or employment. Demonstrated skill, communication, ethics, consistency, and local market conditions all matter.

> **Professional-use notice:** Security testing must stay within systems you own or have explicit written authorization to assess. Standards summaries are educational aids, not certification, legal, or audit advice.

Inside this resource

01 **Role & Outcome Map**
Know the work you are preparing to perform and the evidence employers can evaluate.

02 **12-Month Learning Path**
Progress through foundations, applied practice, portfolio evidence, and job readiness.

03 **Weekly Operating System**
Build consistency with deliberate practice and visible evidence.

04 **Portfolio Projects**
Create proof of skill without exposing secrets, customer data, or unsafe instructions.

05 **Skills & Interview Gates**
Advance only when you can explain, demonstrate, and document the outcome.

06 **Learning Resources & Next 90 Days**
Start small, measure outputs, and adjust based on evidence.

Role & Outcome Map

Know the work you are preparing to perform and the evidence employers can evaluate.

Bug bounty researcher

Entry role focused on supervised execution and documentation.

Vulnerability analyst

Growing role requiring independent investigation and prioritization.

Web penetration tester

Engineering role connecting security controls with systems and software.

Red-team operator trainee

Specialized role reached through deeper practice and delivery experience.

12-Month Learning Path

Progress through foundations, applied practice, portfolio evidence, and job readiness.

Stage 1 · Web Fundamentals

Master HTTP, browser behavior, JavaScript, sessions, APIs, access control, databases, and a repeatable note-taking process.

Stage 2 · Guided Labs

Complete vulnerability-specific labs, explain root cause and remediation, and build checklists from understanding—not payload collections.

Stage 3 · Authorized Programs

Read scope carefully, inventory only allowed assets, respect automation limits, protect data, and communicate professionally.

Stage 4 · Research Depth

Specialize in access control, business logic, APIs, or another domain; compare patterns across technologies and build safe test tooling.

Stage 5 · Red-Team Transition

Add network, identity, cloud, operational security, objectives, detection awareness, evidence, cleanup, and executive reporting.

Weekly Operating System

Build consistency with deliberate practice and visible evidence.

Weekly block	Suggested activity
Concept learning	3–4 hours of focused study and notes
Hands-on practice	5–7 hours in legal labs or datasets
Documentation	One polished diagram, write-up, query, or checklist
Review	Revisit mistakes and create spaced-repetition cards
Community/career	One meaningful interaction, application, or feedback request

Rule: Quality beats streaks. Every practical artifact should show the problem, method, evidence, conclusion, and remediation or improvement.

Portfolio Projects

Create proof of skill without exposing secrets, customer data, or unsafe instructions.

Project 1
Web methodology checklist

Project 2
Three high-quality lab write-ups

Project 3
Safe recon inventory tool

Project 4
Business-logic threat model

Project 5
Professional vulnerability report template

Project 6
Red-team engagement plan and cleanup checklist

Skills & Interview Gates

Advance only when you can explain, demonstrate, and document the outcome.

Foundation gate
Explain core protocols, operating systems, identity, and troubleshooting without relying on memorized tool output.

Practitioner gate
Complete a scoped task, preserve evidence, recognize uncertainty, and recommend an appropriate fix.

Professional gate
Prioritize business impact, communicate to different audiences, handle constraints, and improve team process.

Interview preparation
Use concise STAR examples grounded in your own projects; never claim tools or findings you cannot explain.

Job search
Tailor résumé evidence to role requirements, track applications, request feedback, and iterate monthly.

Learning Resources & Next 90 Days

Start small, measure outputs, and adjust based on evidence.

- HackerOne program policies
- Bugcrowd disclosure guidance
- PortSwigger Web Security Academy
- OWASP Web Security Testing Guide

Days 1–30

Baseline your skills, set up a legal practice environment, and finish one small project.

Days 31–60

Complete a focused learning path and publish a sanitized, reviewed portfolio artifact.

Days 61–90

Run a capstone scenario, practise explanation and interview questions, then begin targeted applications or deeper specialization.



Keep learning. Keep building.

Use this guide as a working plan: practise, document evidence, review outcomes, and improve the next iteration.

mnatech.in @mna_tech_academy +91 9216110094

© 2026 MNA Tech Academy. Original educational resource. Product names and trademarks belong to their respective owners. Verify standards and product details against official sources before production use.