Course 9: API Security for MERN/NestJS

■ Overview

Threat-model driven API security.

■ Prerequisites

- Auth basics

■ Outcomes

Hardened services with defense-in-depth.

■ Benefits

This course empowers learners to build APIs that are resilient against modern attack vectors by applying a threat-model–driven approach to security. Students will gain a practical understanding of the OWASP Top 10 vulnerabilities, learn to secure communications with TLS and mTLS, and implement critical defenses like rate limiting, IP blocking, and bot protection. The course covers validation and sanitization best practices, security headers, and protections against CSRF, XSS, and template injection. Learners will also gain expertise in secure cookies, session management, structured logging, and SIEM integration with PII redaction and alerts. Finally, the course emphasizes operational readiness with incident response strategies, including playbooks and forensics basics. By the end, participants will be able to deliver hardened, defense-in-depth APIs for production environments.

■ Training Key Features

- Threat modeling and OWASP Top 10 foundations
- TLS/HTTPS setup with certificate management and mTLS
- Rate limiting, IP blocking, and bot protection strategies
- Deep dive into Helmet and modern security headers
- Validation and sanitization with Zod & class-validator
- CSRF defense with tokens and double-submit cookie technique
- XSS and template injection protections with React escape model & CSP
- Secure cookie and session management with rotation strategies
- Logging, structured monitoring, and SIEM integration
- Incident response readiness with playbooks and forensics basics

■ Module Breakdown

- Module 1 – Threat Modeling & OWASP ::: threat modeling && OWASP Top 10
- Module 2 – TLS/HTTPS ::: certificates && mTLS overview
- Module 3 – Rate Limiting & Bot Protection ::: rate limiting && IP blocking && bot protection basics
- Module 4 – Security Headers ::: Helmet deep dive && modern headers

- Module 5 – Validation & Sanitization ::: Zod && class-validator
- Module 6 – CSRF ::: tokens && double-submit cookie pattern
- Module 7 – XSS & Template Injection ::: React escape model && CSP strategies
- Module 8 – Cookies & Sessions ::: secure attributes && session rotation
- Module 9 – Logging & SIEM ::: structured logs && PII redaction && alerts
- Module 10 – Incident Response ::: playbooks && forensics basics