Syntho Quest

# API VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

**Duration:** 45 days × 2 hrs/day = 90 hrs

**Goal:** Teach end-to-end API security testing: discovery → static review (specs/code) → dynamic testing → exploitation → PoC → remediation — focused on OWASP API risks and best practises.

**Core API Risk Areas (compact)**

- Broken Object Level Authorization (BOLA) / Broken Access Control
- Broken Authentication & Session Management
- Excessive Data Exposure / Sensitive Data Exposure
- Lack of Resources & Rate Limiting (DoS / abuse)
- Mass Assignment / Insecure Direct Object References (IDOR)
- Security Misconfiguration (CORS, headers, content types)
- Injection (SQL/NoSQL) & Command Injection via APIs
- Improper Assets Management (stale endpoints, old APIs)
- Insufficient Logging & Monitoring
- API-specific issues: Insecure Deserialization, Unprotected Admin Endpoints, Insecure Defaults

**Business Associate:** vivek
**Email:** contact@synthoquest.com
**Mobile:** +91-8333801638 (whats app)