ARMOURINFOSEC®

Hands-On Cyber Security Training · Indore, India

API Security & Advanced API Exploitation

Course Syllabus

Master API security testing, REST API exploitation, GraphQL attacks, SOAP security, JWT vulnerabilities, authorization flaws, SSRF, API reconnaissance, and OWASP API Security Top 10 vulnerabilities through hands-on practical labs and real-world scenarios.

// COURSE INFORMATION

Course Information

DURATION	1 Months / 4 Weeks / 30 Hours
LEVEL	Intermediate to Advanced
MODULES	22
FORMAT	Hands-on Labs / Hybrid (Online + Indore Classroom)

// COURSE OVERVIEW

Course Overview

The API Penetration Testing course is designed for ethical hackers, penetration testers, API security engineers, bug bounty hunters, red team operators, developers, and cybersecurity professionals who want to specialize in modern API security testing. Modern applications heavily rely on APIs for communication between services, mobile applications, cloud infrastructure, and third-party integrations. This course covers REST API exploitation, SOAP security, GraphQL attacks, JWT vulnerabilities, BOLA, BFLA, BOPLA, SSRF, injection attacks, rate limiting bypasses, business logic abuse, and complete OWASP API Security Top 10 methodology.

// LEARNING OBJECTIVES

Learning Objectives

- Conduct comprehensive API security assessments
- Test REST, SOAP, and GraphQL APIs for vulnerabilities
- Exploit all OWASP API Security Top 10 vulnerability categories
- Identify and exploit JWT and OAuth implementation flaws
- Perform BOLA, BFLA, and BOPLA authorization testing
- Conduct API injection attacks (SQL, NoSQL, Command)
- Discover hidden and shadow APIs
- Exploit SSRF and business logic vulnerabilities in APIs

- Bypass rate limiting and resource consumption protections
- Write professional API security assessment reports
- Provide secure API development recommendations

// PREREQUISITES
Prerequisites

- Basic web application knowledge
- Understanding of HTTP and APIs
- Familiarity with Linux and networking
- Basic cybersecurity concepts
- Knowledge of web technologies (JSON, XML)

// MODULE BREAKDOWN
Module Breakdown

01 Introduction to API Penetration Testing

- Overview of API Security
- Importance of API Penetration Testing
- Types of APIs (REST, SOAP, GraphQL)
- Common API Vulnerabilities
- OWASP API Security Risks
- API Attack Surface Analysis

02 Lab Setup & Testing Environment

- Setting Up Testing Environments
- Virtual Machines and Containers
- API Testing Tools Installation
- Network Monitoring Configuration
- Installing Vulnerable Test APIs
- Postman & SoapUI Setup
- Burp Suite API Configuration

03 SOAP API Security

- SOAP Architecture
- WSDL Files and Structure
- SOAP Envelope Structure
- WSDL Enumeration
- XML Injection in SOAP
- SOAPAction Spoofing
- SOAP Parameter Manipulation

04 REST API Security

- REST API Architecture
- Endpoints and Resources
- HTTP Methods (GET, POST, PUT, DELETE)
- Statelessness Concepts

- Endpoint Enumeration
- Parameter Tampering
- HTTP Method Exploitation
- Response Analysis

05 GraphQL API Security

- GraphQL Architecture
- Queries and Mutations
- Schema and Resolvers
- Introspection Queries
- Query Complexity Analysis
- Injection Attacks in GraphQL
- Field-Level Authorization Testing
- Batch Query Abuse

06 API Reconnaissance

- Documentation Review
- Traffic Analysis
- Subdomain Enumeration
- API Discovery Techniques
- API Fingerprinting
- Swagger/OpenAPI Spec Analysis
- Hidden Endpoint Identification

07 Endpoint Analysis & Discovery

- Endpoint Discovery Methods
- Brute Force Enumeration (ffuf)
- Response Code Analysis
- Hidden Endpoint Identification
- API Versioning Exploration
- Wordlist-Based Fuzzing
- Parameter Discovery

08 JWT Vulnerabilities & Exploits

- JWT Structure (Header, Payload, Signature)
- Token Manipulation
- JWT Attacks Overview
- Algorithm Confusion (None Algorithm)
- Signature Verification Issues
- JWK/JKU Header Exploitation
- Token Replay and Refresh Abuse
- JWT Tool Usage

09 API Injection Attacks

- SQL Injection in APIs
- NoSQL Injection
- Command Injection via API Parameters

- LDAP Injection
- GraphQL Injection
- Injection Discovery Techniques
- Automated Injection Testing

10 Broken Object Level Authorization (BOLA)

- Understanding BOLA
- IDOR Vulnerabilities in APIs
- Object Access Manipulation
- Authorization Testing
- UUID Prediction Techniques
- Bulk Data Extraction
- BOLA Remediation

11 Broken Authentication

- API Authentication Mechanisms
- Credential Stuffing
- Brute Force Attacks
- Session Testing
- Token Security Analysis
- API Key Exposure
- OAuth Implementation Flaws

12 Exploiting API Authorization

- Authorization Mechanisms
- Privilege Escalation in APIs
- Role Manipulation
- Access Control Testing
- Horizontal Privilege Escalation
- Vertical Privilege Escalation
- Multi-Tenant Authorization Flaws

13 Broken Object Property Level Authorization (BOPLA)

- BOPLA Concepts
- Property Manipulation
- Sensitive Field Access
- Mass Assignment Vulnerabilities
- Excessive Data Exposure
- Authorization Testing at Property Level

14 Broken Function Level Authorization (BFLA)

- BFLA Concepts
- Function Abuse
- Access Control Testing
- Privileged Function Discovery
- Admin Function Access
- Method-Level Authorization Bypass

15 Rate Limiting & Resource Consumption

- Rate Limiting Concepts
- API Throttling
- Rate Limit Bypass Techniques
- Resource Consumption Vulnerabilities
- Denial of Service via APIs
- Resource Exhaustion
- Abuse Testing Methodology

16 Business Logic & Sensitive Flows

- Business Logic Testing
- Workflow Abuse
- Transaction Manipulation
- Sensitive Flow Exploitation
- Anti-Automation Bypass
- Business Logic Manipulation

17 Server-Side Request Forgery (SSRF)

- SSRF Concepts in APIs
- URL Manipulation
- Internal Resource Access
- Cloud Metadata Exploitation
- Blind SSRF in APIs
- Internal Service Discovery

18 Security Misconfiguration

- Configuration Review
- Security Headers
- Debug Features Exposure
- Misconfigured CORS
- Insecure Defaults
- Verbose Error Responses
- Unnecessary HTTP Methods

19 Improper Inventory & Asset Management

- API Asset Discovery
- Endpoint Inventory
- API Mapping
- Shadow APIs
- Unmanaged Assets
- Legacy API Version Discovery
- Environment Isolation Failures

20 Unsafe Consumption of APIs

- Third-Party API Risks
- API Abuse Patterns
- Unsafe Consumption Patterns

- Dependency Risks
- Supply Chain API Attacks
- Data Validation at Integration Points

21 GraphQL-Specific Attacks

- GraphQL Vulnerabilities
- Deep Query Attacks
- Alias-Based Batching
- Fragment Abuse
- Subscription Exploitation
- Schema Manipulation
- GraphQL DoS

22 Reporting & Remediation

- Documenting API Findings
- Writing Penetration Testing Reports
- Remediation Recommendations
- Risk Prioritization
- Communicating with Developers
- Secure API Development Best Practices
- API Hardening Techniques

// TOOLS & HANDS-ON LABS

Tools & Hands-On Labs

- Purpose-built vulnerable API environments
- SOAP, REST, and GraphQL test targets
- Real-world API scenarios with progressive difficulty
- Postman collections and automated testing scripts
- JWT manipulation lab environment
- OWASP API Security Top 10 challenge labs
- API fuzzing and discovery tools

// TRAINING MODE

Training Mode

Every Armour Infosec course runs as a unified programme delivered in two parallel modes — the same curriculum, the same trainers, the same certification, regardless of how you join.

- ✓ Online Live Classes — real-time, instructor-led, fully interactive sessions
- ✓ On-Premise Classroom Training — in-person at our Indore centre (Sudama Nagar)
- ✓ Both modes run concurrently in every batch; switch between them as your schedule needs
- ✓ Same syllabus, lab access, and certification track for online and on-premise students

// CERTIFICATIONS & CAREER OUTCOMES

Certifications & Career Outcomes

This course aligns with industry-recognised certifications and prepares graduates for offensive-security, application-security, and infrastructure-security roles.

- Supports OSWE exam preparation
- CEH (Certified Ethical Hacker)
- OWASP API Security certification prep
- Bug bounty API methodology
- BSCP (Burp Suite Certified Practitioner)

// ENROL WITH ARMOUR INFOSEC

Enrol With Armour Infosec

Reach out to discuss enrolment, batch schedule, and lab access. Our Indore training centre runs both in-person and live online cohorts with placement assistance.

PHONE	+91 99777 47168
EMAIL	info@armourinfosec.com
ADDRESS	674, Sudama Dwar, Narendra Tiwari Marg, Sudama Nagar, Indore, Madhya Pradesh 452009
WEBSITE	https://armourinfosec.com

Scan to View Course Online

https://www.armourinfosec.com/training/api-security/