

Cyber Security (VAPT) Training

Welcome to TheCodeMacha Cyber Security Training Program, designed to help beginners become skilled VAPT (Vulnerability Assessment & Penetration Testing) professionals.

This course focuses on real-time attack scenarios, practical learning, and industry tools to prepare you for a career in cyber security.

What You Will Learn

- Web Application Security
- API Security Testing
- Mobile Application Pentesting
- Networking & Security Fundamentals
- Real-world vulnerability testing

Course Details

- Course DetailsDuration: 45 Days
- Level: Beginner Friendly
- Mode: Pre-recorded + Practical Learning
- Support: WhatsApp Doubt Support
- Certification: Yes

Tools Covered

Web Application Security

- Burp Suite
- Kali Linux
- Browser DevTools
- Wappalyzer
- Retire.js

API Security

- Postman
- Burp Suite (API testing)

Mobile Pentesting

- MobSF
- JADX
- Frida (Basics)

Networking & Recon

- Nmap
- Wireshark
- Subdomain tools

Cyber Security (VAPT) Training

Master OWASP Top 10 with Real-World Practical Attacks

You will not just learn theory – you will perform real attacks in live environments and understand how hackers think.

Injection Attacks (Critical Vulnerabilities)

- SQL Injection (Error-based, Union-based, Blind)
- Authentication bypass techniques
- Extracting sensitive data from databases

Cross-Site Scripting (XSS)

- Reflected XSS
- Stored XSS
- DOM-based XSS
- Execute real payloads and understand browser-level attacks

CSRF (Cross-Site Request Forgery)

- Perform unauthorized actions using victim sessions
- Understand how attackers exploit authenticated users

IDOR (Broken Access Control)

- Access other users' sensitive data
- Real-world account takeover scenarios

Security Misconfiguration

- Missing security headers
- CORS misconfigurations
- Server information leakage

Vulnerable Components

- Finding outdated libraries (jQuery, etc.)
- CVE identification using real tools
- Understanding real-world exploits

Authentication & Session Attacks

- Login bypass techniques
- Weak session handling
- OTP bypass methods
- Session fixation vulnerabilities

Cyber Security (VAPT) Training

Move Beyond Basics – Think Like a Hacker

SSRF (Server-Side Request Forgery)

- Access internal systems & cloud data
- Exploit backend services

Injection Attacks (Advanced)

- HTML Injection
- Command Injection

Session Hijacking & Account Takeover

- Predictable session attacks
- Real-world account hijacking techniques

Cryptography & Security Fundamentals

- Hashing: MD5, SHA256, SHA512
- Encryption concepts
- TLS & HTTPS security testing

Business Logic Attacks (Real Industry Scenarios)

- Price manipulation
- Coupon abuse
- Workflow bypass
- These are real bugs companies pay for

Cyber Security (VAPT) Training

Complete VAPT Coverage (Web + API + Mobile + Network)

API Security Testing

- Testing APIs using Postman
- Broken authentication & authorization
- Sensitive data exposure
- Real API attack scenarios

Mobile Application Pentesting

- Reverse engineering APKs using JADX
- Static analysis using MobSF
- Basic runtime testing techniques

Networking & Infrastructure Basics

- TCP/IP fundamentals
- Ports & protocols
- Packet analysis using Wireshark
- Port scanning using Nmap

Hands-On Practical Training

- Real vulnerable labs
- Live attack simulations
- Bug hunting mindset development

Cyber Security (VAPT) Training

From Beginner to Job-Ready VAPT Professional

Industry Tools You Will Master

- Burp Suite
- Kali Linux
- Postman
- MobSF
- JADX
- Nmap
- Wireshark

After Completing This Course, You Will Be Able To:

- Perform complete VAPT on web applications
- Identify real-world vulnerabilities
- Think like an ethical hacker
- Use professional cybersecurity tools
- Understand both attack & defense techniques

Career Opportunities

After completion, you can apply for:

- Penetration Tester
- VAPT
- Bug Bounty Hunter
- Start your career as a Fresher Cyber Security Professional

Support & Learning System

- WhatsApp doubt support
- Help with practical understanding
- Real-world scenario discussions

Important Information

- 100% Beginner Friendly
- No prior coding required
- Training via pre-recorded videos
- Learn at your own pace