SKILLFORGE
ACADEMY

BUILD SKILLS. FORGE SUCCESS.

VAPT COURSE

Vulnerability Assessment & Penetration Testing

Version @2025

PROGRAMME OVERVIEW

Cybersecurity threats are evolving faster than ever. According to global reports, the cybersecurity market is expected to cross $180+ billion by 2024, with over 1 million job opportunities in India by 2027.

SkillForge Academy’s VAPT Training Programme equips you with practical skills to identify, exploit, and secure vulnerabilities across networks, systems, and applications. This course is designed to transform you into a job-ready cybersecurity professional capable of handling real-world attacks.

SKILLFORGE ACADEMY
BUILD SKILLS. FORGE SUCCESS.

ABOUT SKILLFORGE ACADEMY

SkillForge Academy is a cybersecurity training and consulting institute built by experienced security professionals with 6+ years of expertise.
We are dedicated to:

- Delivering hands-on ethical hacking training aligned with industry standards.
- Providing placement assistance and internships with real-world projects.
- Mentoring students in bug bounty hunting and competitive cybersecurity challenges.

Version @2025

WHY CHOOSE SKILLFORGE FOR VAPT TRAINING?

- 100% Practical-Oriented Learning – Perform real attacks in labs, not just theory.

- Comprehensive Curriculum – Cover network, web, mobile, and advanced exploitation.

- Expert Trainers – Learn from industry professionals actively working in cybersecurity.

- 24/7 Cloud Labs – Pre-configured labs (Kali Linux, Windows, web apps) accessible anytime.

- Placement & Internship Support – Guidance for jobs, bug bounties, and certifications.

VAPT TRAINING COURSE CONTENT

CYBER SECURITY:

- Introduction to Cyber Security
- Types of JOBS
- Types of Hacking or testing
- Ethical Hacking
- Communication Model
- DNS, IP Types and introduction
- PORTS & Usage
- Cryptography
- VAPT Introduction
- VAPT Process we follow

Basics to WEB VAPT:

- WEB Communication Model
- Request & Response Components
- Burpsuite tool Walkthrough
- Recon of Web application (Wappalyzer, shodan)
- Vulnerability Severity (CIA)
- Report Pattern
- CWE
- Zero Day Vulnerability
- HTTP & HTTPS
- Types of Web Applications

VAPT TRAINING COURSE CONTENT

WEB APPLICATION VAPT:

- OWASP Top 10 List
- Session Vulnerabilities
- Password Vulnerabilities
- Authentication Vulnerabilities
- Authorization Vulnerabilities
- Security Misconfiguration Vulnerabilities
- XSS Vulnerabilities
- Business Logic Vulnerabilities
- Injections (SQL, LDAP, COMMAND & XML)
- Host Header Vulnerabilities
- Input Vulnerabilities (XSS, HTML, CSS, Iframe)
- CSRF
- SSRF
- Broken Access Control Vulnerabilities
- IDOR
- Sensitive Data Exposure Vulnerabilities
- ASPX, PHP, TOMCAT Vulnerabilities
- Rate Limiting, Brute Force Vulnerabilities
- User Enumeration Vulnerabilities
- Privilege Escalation
- Low Vulnerabilities List
- Remote Code Execution & File Upload Vulnerabilities
- Complete Checklist
- Automation Tools intro & Walkthrough

VAPT TRAINING
COURSE CONTENT

NETWORK VAPT:

- OSI Model
- PROTOCOLS
- TCP
- IP
- Host Discovery, Port scanning & NMAP Tool
- Nessus & Nexpose Tools
- Metasploit
- Firewalls, WIFI
- DNS Spoofing
- SMB Relay Attack
- Password cracking
- Checklist for Network VAPT

VAPT TRAINING COURSE CONTENT

SKILLFORGE ACADEMY

BUILD SKILLS. FORGE SUCCESS.

MOBILE VAPT(ANDROID):

- OWASP Top 10 List
- Mobsf
- Emulator Setup
- Reverse Engineering
- Static Analysis
- Insecure Data storage
- Dynamic analysis
- Checklist for Mobile VAPT
- Intro to IOS VAPT

API VAPT:

- Types of API
- Setup of Postman & SOAP
- Session Vulnerabilities
- Auth Vulnerabilities
- Sensitive data exposure Vulnerabilities
- Security Misconfiguration Vulnerabilities
- Rate limiting
- Injections
- Input Vulnerabilities
- JWT Vulnerabilities
- Checklist For API VAPT

SOURCE CODE REVIEW (VAPT):

- SCR Introduction
- Manual & Automated types
- OWASP List
- Language Specific Vulnerabilities
- Encoding Vulnerabilities
- Input validation Vulnerabilities
- Business logic Vulnerabilities
- Authentication & Authorization Vulnerabilities
- Checklist for SCR

Bug Bounty:

- Introduction of Bugbounty
- Profile Setup
- Walkthrough
- Reports & Access
- Few tips Bypass techniques
- Approach Methods

VAPT TRAINING COURSE CONTENT

Tools List:

- Burpsuite
- Wappalyzer,Shodan, Cookies Editor
- Acunetix, Net Sparker
- Mobsf, Ostra Labs
- JADX
- Mobile emulators: Nox Player & Genymotion
- WordPress Scanner
- NMAP
- Metasploit
- Nexpose & Nessus
- POSTMAN & SOAP
- OWASP ZAP
- SQL MAP
- Wireshark
- Jhon the ripper
- Checkmarx
- Github
- Kalilinux

KEY TAKEAWAYS

By the end of this course, you will be able to:

- Perform end-to-end VAPT assessments on real networks and applications.
- Understand offensive & defensive cybersecurity strategies.
- Create detailed vulnerability reports for enterprises.
- Gain exposure to bug bounty methodologies.
- Be prepared for job interviews and certifications (CEH, OSCP, etc.).

SKILLFORGE
ACADEMY

BUILD SKILLS. FORGE SUCCESS.

CERTIFICATION

On successful completion, you will receive a SkillForge Academy VAPT Certification recognized by industry partners. This validates your expertise and makes you job-ready in cybersecurity.

SKILLFORGE
ACADEMY

BUILD SKILLS. FORGE SUCCESS.

COURSE DETAILS

Duration: 2 Months(60-70 Days)

Mode: Online + Offline (Hybrid)

Fees: ₹19,999 (EMI Options Available)

Contact Us

📞 +91 8074039665

✉️ theskillforgeacademy@gmail.com

THANK YOU!

Version @2025