SECURE FLOW INFOTECH
Secure Solutions. Smart Flow. Seamless Future.

CYBERSECURITY VAPT

Vulnerability Assessment and Penetration Testing (VAPT)

Topics Covered

- Web Application Security
- API Security Testing
- Mobile Application Security Testing
- Network Pentesting

1. Web Application Security:

Basics:

- 2-Tier architecture
- 3-tier architecture
- HTTP vs HTTPS
- Request and Response Headers
- API Methods
- Status Codes

Tools for web:

- 2-Tier architecture
- 3-tier architecture
- HTTP vs HTTPS
- Request and Response Headers
- API Methods
- Status Codes

Methodology for Web Application Security Testing - Owasp Top 10 2021/2025:

2. API Security Testing:

Basics:

- What is API
- How do APIs work?
- Types of API
- Importance of APIs

Tools for API:

- Postman
- Soap UI
- Postman integration with Burp suite
- Soap UI integration with Burp suite

Methodology for API Security Testing - Owasp Top 10 2019/2023

3. Mobile Application Security:

Basics:

- What is Android
- What is APK
- Android structure
- Android Fundamentals
- Android Components
- Android File System
- Reverse Engineering

Testing Requirements:

- Physical Device
- Emulators (Virtual Mobile Device)
- Memu Play
- Android Studio
- Genymotion
- Nox

Tools for Android

- MobSF
- Jadx-gui
- APK Tool
- ADB
- Magisk
- Frida
- Objection

Methodology for Mobile Security Testing - Owasp Top 10 2016/2024

Comparison Between 2016-2024		
OWASP-2016	OWASP-2024-Release	Comparison Between 2016-2024
M1: Improper Platform Usage	M1: Improper Credential Usage	New
M2: Insecure Data Storage	M2: Inadequate Supply Chain Security	New
M3: Insecure Communication	M3: Insecure Authentication / Authorization	Merged M4&M6 to M3
M4: Insecure Authentication	M4: Insufficient Input/Output Validation	New
M5: Insufficient Cryptography	M5: Insecure Communication	Moved from M3 to M5
M6: Insecure Authorization	M6: Inadequate Privacy Controls	New
M7: Client Code Quality	M7: Insufficient Binary Protections	Merged M8&M9 to M7
M8: Code Tampering	M8: Security Misconfiguration	Rewording [M10]
M9: Reverse Engineering	M9: Insecure Data Storage	Moved from M2 to M9
M10: Extraneous Functionality	M10: Insufficient Cryptography	Moved from M5 to M10

4. Network Pentesting:

Basics:

- What is Network
- Types of Network Pentesting
- Common Protocols
- Ports and Services
- IP Addressing
- TCP and UDP
- Three-Way Handshake
- OSI Layer Model
- TCP/IP Model
- Network Devices

Network Pentesting Methodology:

- Reconnaissance
- Scanning
- Enumeration
- Exploitation
- Post-Exploitation
- Reporting

Tools:

- Nmap
- Nessus
- Wireshark
- Metasploit Framework
- Netcat
- Hydra
- John the Ripper

Deep Dive – For Each Topic

- Description (What is the issue and how to find)
- Impact (What is the risk of the issue)
- Solution (How to fix the issue)
- Reference (To read about the issue)
- Practical Labs

Services we will provide with the course:

- Daily Class Notes
- Class Recordings
- Resume Preparation
- Interview Preparation
- Mock Interview
- Daily Assessments

Each and every session will be conducted live

Phone: **+91 91884 94949 / +91 91339 19666**

Website: **https://secureflowinfotech.com**

SECURE FLOW
INFOTECH
Secure Solutions. Smart Flow. Seamless Future.