ClockXInfosec Solutions

CYBERSECURITY TRAINING & PLACEMENT

OFFICIAL PROGRAM BROCHURE

Fresher VAPT Training Program

A structured, industry-oriented program that prepares beginners for junior Vulnerability Assessment & Penetration Testing roles through live teaching, hands-on practice on **modern real-time applications**, and a clear path to professional readiness.

Duration **3 months**	Schedule **Saturday & Sunday**
Session length **4 hours / day**	Live training **~96 hours**
Format **Live classes (no recordings)**	Focus **Fresher / Junior VAPT**
Trainers **Certified professionals (5+ yrs)**	Course & labs **Industry-built curriculum**

For students and parents · ClockXInfosec Solutions
Official: **8828135939** (Call + WhatsApp)

1. About ClockXInfosec Solutions

ClockXInfosec Solutions trains fresh graduates and beginners for **entry-level cybersecurity careers**, with a strong focus on practical VAPT. Students learn in live sessions and immediately apply skills on **labs built as modern, real-time applications** — similar to the applications used in real organisations.

> **Our standard is skill.** We prepare students thoroughly, measure progress honestly, and provide placement support for candidates who meet the ClockXInfosec Solutions quality bar.

2. Trainers & Industry Expertise

Teaching, course design, and hands-on labs are led by **cybersecurity professionals with 5+ years of industry experience** and **multiple relevant certifications**. Students learn what companies actually expect from junior VAPT roles — not only theory.

3. Program Snapshot

Item	Detail
Program	Fresher VAPT Training Program
Organisation	ClockXInfosec Solutions
Duration	3 months (~12 weekends)
Class days	Saturday and Sunday
Weekend only	4 hours each day (8 hours per weekend)
Total live hours	Approximately 96 hours
Practice between weekends	About 2–4 hours per week
Delivery	Live teaching + live labs + doubt clearing
Lab style	Modern real-time applications (private lab access per student for web practice)
Module live tests	Live practical test after Networking, OS, and Web modules
Completion	Final Clearing Exam + professional report standard
Placement	Merit-based after exam, report quality, and interview readiness

4. What Students Achieve

- Strong networking foundation for cybersecurity work
- Practical use of tools such as Wireshark, Nmap, and vulnerability scanners
- Hands-on Linux and Windows security enumeration skills
- In-depth web application security testing across **OWASP Top 10 (2025)** and related vulnerability classes
- Working knowledge of API security, mobile security basics, and responsible AI use
- Ability to write a clear, professional security assessment report
- Confidence for junior VAPT / AppSec interviews

5. Live Labs on Modern Real-Time Applications

ClockXInfosec Solutions labs are designed around **realtime modern applications** — with login, user roles, forms, uploads, workflows, and APIs — so students practise the way junior professionals work.

- Student opens the weekend challenge on the ClockXInfosec Solutions learning portal
- Starts a private lab environment for practice
- Works only inside authorised ClockXInfosec Solutions labs
- Submits checkpoints; cohort leaderboard supports healthy competition
- Stops the lab when finished

6. Curriculum Overview

Stage	Focus	Live hours
Networking for Cybersecurity	Foundations + scanning tools	16h
Linux & Windows	OS skills for security testing	16h
Web Application Security	Full OWASP-depth web testing (core)	40h
API, Mobile & AI	API OWASP, mobile intro, AI awareness	12h
Reporting	Professional report writing	4h
Capstone & Final Exam	End-to-end practice + clearing exam + interview prep	8h+

12-weekend roadmap

Each weekend is **Saturday + Sunday**, **4 hours per day** (8 live hours). Detailed topic lists for each stage continue in the sections below.

Weekend	Focus	Block
1	Network foundations for cybersecurity	Networking (16h)
2	Network tools — Nmap, Wireshark, Nessus triage + asset inventory	
3	Linux enumeration for offensive basics	Linux & Windows (16h)
4	Windows enumeration (CMD + PowerShell)	
5	Methodology, Burp Suite & recon	Web App Security (40h)
6	Authentication, session & access control	
7	Injection family (SQLi, command, SSTI awareness)	
8	XSS, CSRF, SSRF, upload & business logic	
9	Modern web topics + module live practical	
10–11a	OWASP API Top 10, Mobile basics, AI / OWASP LLM	API · Mobile · AI (12h)
11b	Professional reporting (mini engagement write-up)	Reporting (4h)
12+	Capstone, Final Clearing Exam & mocks until job-ready	Capstone & placement (8h+)

Module live tests run after Networking, OS, and Web. Exact test content is shared only in class.

7. Networking for Cybersecurity (16 hours)

Network Foundations

- Why networking matters in cybersecurity
- Network types and topologies (LAN / WAN / WLAN)
- Hub, Switch, Router, NIC, Access Point, Gateway, Firewall
- MAC vs IP, ARP basics
- OSI model and TCP/IP model
- IPv4, public/private IP, DHCP, NAT, basic subnetting
- Common ports and services
- Cleartext vs encrypted traffic
- TCP vs UDP, three-way handshake
- DNS, HTTP, HTTPS / TLS basics, ICMP
- End-to-end traffic path through a network

Live lab — what students practise

- Label a real lab network diagram (hub, switch, router, firewall, gateway)
- Capture live traffic with Wireshark and identify MAC, IP, ports, and the TCP handshake
- Compare clear HTTP traffic vs HTTPS and explain why encryption matters
- Map the lab subnet: hosts, segments, and default gateway
- Submit annotated screenshots and a simple topology sketch

Network Tools & Vulnerability Scanning

- Host discovery and port-scanning methodology
- Nmap (host, port, service, scripts)
- Netcat, dig / nslookup, traceroute, ping
- Banner grabbing and result triage
- Wireshark filters and stream analysis
- Vulnerability scanning concepts and false-positive handling
- Nessus (licensed) result reading and triage
- Professional asset inventory preparation

Live lab — what students practise

- Discover live hosts on a multi-host office-style lab network
- Run structured Nmap scans (ports, services, versions) — not blind scanning
- Use supporting checks: ping, traceroute, DNS lookup, banner review
- Run a scoped vulnerability scan and triage results for false positives
- Build a professional asset inventory sheet (host, IP, ports, service, confirmed notes)

Module live test: After this Networking module, students take a live practical test before moving to the next stage. (Test details are shared only in class.)

8. Linux & Windows (16 hours)

Linux

- Linux structure and important directories
- Shell basics and system information
- Files, search, pipes, and filters
- Users, groups, and permissions
- Packages, processes, and services
- Linux networking commands (IP, ports, curl, SSH)
- Basic log review for security work

Live lab — what students practise

- Log into a live Linux lab system and confirm identity / system information
- Navigate important directories and search for interesting files
- Enumerate users, groups, and file permissions
- Check running processes, services, and listening network ports
- Review basic logs and fill a structured Linux enumeration checklist

Windows

- Windows structure and important paths
- File system and share permissions
- Registry awareness
- Users, groups, privileges, services, and processes
- Command Prompt and PowerShell enumeration
- WMI / MMC awareness, Event Viewer overview
- SMB shares and RDP awareness (lab environment)

Command Prompt: hostname, whoami, systeminfo, net user, net localgroup, dir, ipconfig, ping, netstat, net share, tasklist, sc query, and related commands.

PowerShell: Get-LocalUser, Get-LocalGroup, Get-Process, Get-Service, Get-NetIPAddress, Get-NetTCPConnection, Test-NetConnection, Resolve-DnsName, Get-SmbShare, and related cmdlets.

Live lab — what students practise

- Enumerate a live Windows lab system using Command Prompt
- Repeat the same checks using PowerShell cmdlets
- List local users/groups, services, processes, and network listeners
- Inspect shares and understand permission basics on a real share
- Peek Event Viewer / security logs and complete the full OS checklist

Module live test: After the Linux & Windows module, students take a live practical test before starting Web Application Security. (Test details are shared only in class.)

9. Web Application Security (40 hours) — Core Module

This is the heart of the program. Students train across **almost the full set of web vulnerability classes** expected for junior VAPT work, mapped to **OWASP Top 10 (2025)**, and practised on a **modern real-time ClockXInfosec Solutions web application** (private lab per student).

OWASP Top 10 (2025) — where each category is taught

ID	Category	Main weekends
A01	Broken Access Control (incl. IDOR, CSRF, SSRF, path traversal, open redirect)	6, 8, 9
A02	Security Misconfiguration	5, 9 (lite)
A03	Software Supply Chain Failures	9 (lite)
A04	Cryptographic Failures	6, 9 (lite)
A05	Injection (SQLi, XSS, command, SSTI, etc.)	7, 8
A06	Insecure Design / business logic	8
A07	Authentication Failures	6
A08	Software or Data Integrity Failures	9 (JWT lite)
A09	Security Logging and Alerting Failures	9 (awareness)
A10	Mishandling of Exceptional Conditions (errors, fail-open, bad exception handling)	5, 9 (lite)

Methodology, Burp Suite & Reconnaissance

- Engagement scope and professional testing rules
- HTTP for testers (methods, status codes, headers, cookies)
- Threat modelling basics
- Burp Suite setup and core tools
- Application mapping and content discovery
- Misconfiguration and error-handling signals

Live lab — what students practise

- Start a private modern ClockXInfosec Solutions web application lab
- Configure Burp Suite proxy and confirm HTTPS interception
- Browse as guest and as logged-in user; map pages, forms, and APIs
- Build an endpoint sheet (method, parameters, auth vs unauth)
- Note misconfiguration and error signals for later testing

Authentication, Session & Access Control

- Authentication failures and session management
- Cookie security flags
- Broken access control, IDOR, privilege escalation
- Open redirect awareness
- Cryptographic failure awareness
- Evidence standards for reporting

Live lab — what students practise

- Test login, session cookies, and logout / timeout behaviour
- Check cookie security flags and session handling
- Attempt IDOR / privilege checks between user roles
- Capture request/response evidence in Burp Suite
- Write at least two findings with business impact and OWASP mapping

Injection & Database Issues

- SQL injection and confirmation methods
- Database impact and remediation guidance
- Command injection
- SSTI, XXE, and related injection awareness
- Validation vs encoding; WAF awareness

Live lab — what students practise

- Test search and form inputs for SQL injection on the modern app
- Confirm findings carefully (avoid false positives)
- Demonstrate database / application impact with clear evidence
- Practise command-injection awareness where the lab allows
- Write remediation notes a developer can actually implement

Client-Side, File & Business Logic Issues

- XSS (reflected, stored, DOM overview)
- CSRF and SSRF
- Insecure file upload, path traversal, LFI basics
- Business logic / workflow abuse
- Clickjacking and HTTP method tampering awareness

Live lab — what students practise

- Test for XSS in profile/comment/input fields
- Check CSRF on state-changing actions
- Test SSRF / URL-fetch features where present
- Attempt insecure file upload and path traversal checks
- Abuse a business workflow (price, steps, or role logic) and document impact

Modern Web Topics

- CORS
- JWT pitfalls
- Rate limiting and brute-force controls
- Mass assignment
- API-style endpoints inside web apps
- Supply chain, logging/alerting, and exceptional-condition awareness
- Retest mindset

Live lab — what students practise

- Work on a fresh modern application instance under a short time scope
- Test CORS, JWT handling, rate limiting, and mass assignment
- Revisit earlier vulnerability classes and validate findings with evidence
- Write clear finding titles, steps, impact, and remediation
- Practise retest mindset — confirm and re-verify before marking complete

Module live test: After the Web Application Security module, students take a live practical test before moving to API / Mobile / AI. (Test details are shared only in class.)

10. API, Mobile & AI Basics (12 hours)

- REST / GraphQL surface awareness
- OWASP API Top 10 overview
- Differences between API testing and classic web form testing
- Mobile security basics (traffic intercept concept, insecure storage overview)
- Responsible AI use in security work
- OWASP LLM / GenAI Top 10 awareness

Live lab — what students practise

- API station: test object access and role checks on JSON APIs (BOLA / BFLA style)
- Mobile station: install a sample app path, intercept traffic, note insecure storage basics
- AI station: draft recon/remediation notes with AI using sanitized lab data only
- Human verification checklist — student confirms AI output before trusting it
- Map at least three API OWASP categories to endpoints seen in the web lab

11. Reporting, Capstone & Final Assessment

Professional Reporting (4 hours)

- Evidence standards (request/response, screenshots, impact, remediation)
- Report structure used in industry
- Severity language for clients and hiring managers

Live lab — what students practise

- Convert practical findings into the ClockXInfosec Solutions report template
- Write executive summary, scope, methodology, and detailed findings
- Attach evidence (screenshots / request-response) for each issue
- Add severity, business impact, and clear remediation steps
- Complete risk matrix and prepare the report for trainer review

Capstone, Final Clearing Exam & Interview Preparation

- **Capstone:** End-to-end practice on a modern real-time application — test, evidence, report draft, trainer review
- **Final Clearing Exam:** Mandatory end-of-program practical examination and short viva — must clear to complete the program
- **Interview preparation:** Technical and HR-style mock interview practice until interview-ready

Note: Module live tests (after Networking, OS, and Web) plus the Final Clearing Exam confirm progress. Exact test content is not published in this brochure and is shared during the program.

12. Placement Support — ClockXInfosec Solutions Policy

- Placement support is **merit-based**, not automatic
- Student must pass the Final Clearing Exam
- Student must meet the professional report standard
- Student must clear ClockXInfosec Solutions interview-readiness standards
- Certification guidance may be provided for resume screening; interviews are won through practical skill

13. Student Requirements

- Laptop suitable for browser-based labs and Burp Suite
- Stable internet for Saturday–Sunday live classes
- ClockXInfosec Solutions student account for lab access
- Regular live attendance and consistent practice

14. Code of Conduct

- Attend live classes and complete labs honestly
- Practice only on labs provided by ClockXInfosec Solutions
- Never test any outside website, application, or network without written permission
- Respect classmates and healthy competition rules
- Use only licensed tools as guided by trainers

Violation of ethical or lab rules may result in removal from the program and loss of placement support.

15. Contact

For batch dates, fees, and admissions, please contact ClockXInfosec Solutions. Students and parents are welcome to ask questions before enrollment.

> **Official number:** 8828135939 (Call + WhatsApp)

ClockXInfosec Solutions — Fresher VAPT Training Program
Official: 8828135939 (Call + WhatsApp)
Live teaching · Modern real-time application labs · Industry-aligned curriculum · Merit-based placement support