

Programme on

VAPT & Continuous Security Validation

Programme Coordinator: [Dr. V. Radha](#)

July 16 - 18, 2025



INSTITUTE FOR DEVELOPMENT AND RESEARCH IN
BANKING TECHNOLOGY, HYDERABAD
(ESTABLISHED BY RESERVE BANK OF INDIA)



Introduction

Vulnerability Assessment and Penetration Testing (VAPT) is crucial for BFSI to proactively identify and address security risks before they are exploited. A VAPT course equips individuals with the knowledge and skills to perform VAPT, including identifying vulnerabilities, conducting penetration tests, and developing mitigation strategies.

Continuous Security Validation (CSV) is an important component of cybersecurity because it provides a proactive and automated approach to testing security controls, identifying vulnerabilities, and ensuring they remain effective in the face of evolving threats.

While VAPT helps in placing right security controls as risk mitigation strategy, the CSV ensures that the security controls are functioning effectively and efficiently.

Objectives

The objective of this programme is to provide information about the latest security validation methods, practices and platforms that help in carrying out security validation. In turn, these steps will help organisations to strengthen their cyber security precautions.

Contents

- ★ **Introduction to Cyber Security:**
 - Overview of cyber security landscape
 - Understanding vulnerabilities and exploits
- ★ **Security Validation – The Past:** Focusses on the methods practiced in the past like the VAPT, Patching; its pros and cons
- ★ **Security Validation – The Present:** Spotlights the present methods such as:
 - Red Team and Blue Team Exercises,
 - Threat Hunting
 - BAS – Breach and Attack Simulation; its pros and cons
- ★ **Security Validation – The Future:** A system that continuously monitors and tests the security controls in the enterprise. Also highlights how CSV is different and the ways and means to carry CSV

- ★ The Programme also features the topics like
 - Vulnerability Assessment Methodologies
 - Reconnaissance and Information Gathering
 - Scanning and Enumeration
 - Understanding Exploit Frameworks (e.g., Metasploit)
 - Exploiting Vulnerabilities to gain Unauthorized Access
 - Privilege Escalation and Maintaining Access
 - Post-exploitation Techniques (e.g., Data Exfiltration, Lateral movement)
 - OWASP Top10 Vulnerabilities
 - Web Application Scanning and Testing Methodologies
 - Exploiting Common Web Application Vulnerabilities (e.g., SQL injection, XSS)
 - Wireless Network Penetration Testing
 - Understanding Social Engineering Tactics and Techniques
 - Physical Security Assessments and Techniques
 - Vulnerability Management and Reporting

Who can Participate?

Officers from Banks and Financial Institutions managing Cyber Security / IT, etc.

End Use

This Programme is designed to provide the participants with the latest know-how so as to help them significantly improve the security of their enterprise and achieve better cyber security maturity levels

Programme Coordinator

Dr. V. Radha, Associate Professor. e-mail: vradha@idrbt.ac.in.

Accommodation

Participants will be provided Air Conditioned Single Occupancy accommodation in IDRBT, Hyderabad, with all cafeteria facilities. The Participants can check-in on the evening of the day before the commencement of the programme and can check-out after completion of the programme on the same day (or) in the morning of the next day of the programme.



Fee Details

Domestic Participants from

- ★ RRBs & Coop. Banks : Rs. 44, 840/- (Rs. 38, 000/- + 18% GST)
- ★ All other Banks & FIs : Rs. 53, 100/- (Rs. 45, 000/- + 18% GST)

The fees for our programmes can be remitted through NEFT and the bank account details for fee payment are here under:

Account Name : IDRBT
Bank : Axis Bank Limited
Branch : Humayun Nagar (Mehdipatnam Ring Road) Branch,Hyd.
Account Number: 426010100018823
IFSC Code : UTIB0000426
GSTIN : 36AAAAI0204K1Z4.

Nominations

Nominations may please be sent to us latest by **JULY 01, 2025** by email to hunar@idrbt.ac.in. Please note that no nominations will be accepted after this date. This measure is envisaged to further improve the quality and learning outcomes of the programmes based on participants' profile and requirements.

While nominating, please provide the details of the participants (Name, Designation, Bank, Mobile No / Phone No., email address) along with the nominating authority details (Name, Designation, Bank, Mobile No / Phone No., email address, Fee billing address, GST No. of the bank).

Contact Us

Please contact our Programme Office for organising Customized Programmes and/or any other queries related to programmes at hunar@idrbt.ac.in or call us on +914023294121/24/25.