

Programmes Scheduled in February 2023

S. No.	Programme	Date	Coordinator
1	IT Operational Risk Management	06 - 08	Dr. N. P. Dhavale
2	Biometric Payment Systems	06 - 08	Dr. MVNK Prasad
3	Secure Coding Practices	06 - 08	Dr. V. Radha
4	Robotic Process Automation	13 - 15	Dr. Rajarshi Pal
5	Big Data and Cloud	13 - 17	Dr. P. Syam Kumar
6	Payment Systems	13 - 17	Dr. Susmita Mandal
7	Server-less Compute Platforms	20 - 22	Dr. Subhrendu
8	Mobile Application Development and Security Testing	20 - 24	Dr. V. N. Sastry
9	Blockchain for Banking	Feb 27 - Mar 01	Dr. Susmita Mandal
10	Information Systems Control and Audit	Feb 27 - Mar 03	Dr. Dipanjan Roy
11	IT Project Management & Vendor Management	Feb 27 - Mar 03	Dr. Abhishek Thakur
12	Fraud Analytics	Feb 27 - Mar 03	Dr. Mridula Verma

Please visit our website for more details at : <https://www.idrbt.ac.in/offline-programmes>

Programme Office

Please contact our Programme Office for organizing Customized Programmes and/or any other queries related to programmes:

Mr. K. Srinivas
Administrative Executive

Mr. D. Chaitanya
Administrative Executive

Institute for Development and Research in Banking Technology
Castle Hills, Road No. 1, Masab Tank, Hyderabad - 500 057, India.

Phone: +91-40-2329 4121 / 22 / 24 / 25

Web: www.idrbt.ac.in **E-mail:** program@idrbt.ac.in

SECURE CODING PRACTICES

Coordinator: **Dr. V. Radha**

FEBRUARY 06 – 08, 2023



Secure Coding Practices

February 06 – 08, 2023

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

Introduction

With lots of digitisation around, banks are under stress to open APIs, develop new Applications for customers as well as employees around their core banking. Building new apps around core banking without proper understanding of OWASP top 10 security vulnerabilities like SQL Injection, Remote Code Execution etc might put the bank in higher risk zone. Whether the bank develops the application on its own or buys it, it is advisable for the bankers to understand the OWASP vulnerabilities, how do they manifest and what are the remedial measures. For majority of the attacks, bad programming is the sole source of problem. Security experts deploy remedial measures across the entire enterprise network stack right from Web application firewalls, to end-point security. It is like making the outer wall stronger to secure the weak inner applications. Dependency on majority of the present day security solutions around network stack, can be reduced if the programs are written with security in mind.

Objective

To bring awareness about OWASP top 10. Discuss and demonstrate the remedial measures; Automated testing of applications; Code Scanning and Code Analysis.

Contents

- * OWASP Top-10 – Overview
- * PKI for Information Security in Banking Services
- * SSL
- * Web Application Security
- * Cross Site Scripting and Remedial Measures
- * Database Security
- * SQL Injection and Remedial Measures
- * Remote Code Execution – Buffer Overflow Attacks and Remedial Measures
- * Session Hijacking and Remedial Measures
- * Insecure Authentication and Remedial Measures
- * Insecure Data Storage and Remedial Measures
- * Weak Encryption and Remedial Measures

End Use

Participants would be able to appreciate the RCA of vulnerabilities and act accordingly to strengthen the overall IT environment in all its dimensions: Data, Applications and Technologies.

Faculty

Faculty of IDRBT, Guest Speakers from the Industry & Practitioners.

Who Can Participate?

Developers, Inspection officials as well as officers in IT function involved in design, deployment and maintenance of information systems.

Fee Details

Domestic Participants from

- * RRBs & Coop Banks : Rs. 41,300/- (Rs. 35,000/- + 18% GST)
- * All other Banks & FIs: Rs. 46,020/- (Rs. 39,000/- + 18% GST)

Foreign Participants from

- * SAARC Countries : US \$708/- (US \$ 600/- + 18% GST)
- * Other Countries : US \$ 1062/- (US \$ 900/- + 18% GST)

The fees for our programmes can be remitted through NEFT and the bank account details for fee payment available at: <https://bit.ly/3PXGK35>.

Bank Account Details for Remittance of Fees

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

Nominations

Nominations should be sent to us latest by **JANUARY 31, 2023** by email to program@idrbt.ac.in

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, Fees billing address, GST No. of the bank).

Venue & Timings of Programme

Venue: IDRBT **Timings:** 9.30 AM to 5.30 PM

How to Reach IDRBT

A major landmark near Masab Tank flyover is NMDC. IDRBT is located just behind NMDC. Google Pin: <http://bit.ly/IDRBT>

Accommodation and Travel Plans

The boarding & lodging arrangements will be made at IDRBT, Hyderabad. The participants will be provided single occupancy a/c rooms.

Check-in : From 3.00 PM on Sunday, February 05, 2023.

Check-out : 7.00 AM on Thursday, February 09, 2023.