

MDP for Secure Coding Practices for Banking

DURATION: (4 days)

PROGRAM CONTEXT

This program focuses on secure coding practices tailored for the banking and financial services sector, where data protection, regulatory compliance, and application security are paramount. It equips developers and security professionals to build secure, resilient, and compliant financial applications.

Covering secure design principles, OWASP and CWE vulnerabilities, encryption, authentication, and third-party risk management, the program emphasizes integrating security throughout the development lifecycle. Through banking-focused use cases, participants learn to reduce vulnerabilities, prevent breaches, and protect sensitive financial data while supporting digital innovation.

PROGRAM OBJECTIVES

- Apply **secure input validation and output encoding** techniques,
- Implement strong **authentication and authorization controls**, including secure password policies, MFA, RBAC, and session management
- Ensure robust **data protection practices**, including encryption at rest and in transit, secure APIs, and safe token handling
- Design secure **error handling and centralized logging** to prevent information leakage
- Develop **secure APIs** using JWT/OAuth basics, rate limiting, and strict input validation
- Apply **secure coding standards and best practices** through structured code reviews

PROGRAM MODULES

1. OWASP Top 10

- Injection attacks
- Broken Authentication
- Sensitive Data Exposure
- XSS
- Insecure Deserialization
- Security Misconfiguration

2. Input Validation & Output Encoding

- Prevent SQL Injection
- Prevent XSS
- Validate all user inputs
- Use prepared statements

3. Authentication & Authorization

- Strong password policies
- MFA concepts

- Role-based access control
- Secure session handling

4. Data Protection

- Encryption at rest & in transit
- Secure APIs
- Token handling
- Avoid logging sensitive data

5. Error Handling & Logging

- Safe error messages
- Centralized logging
- Monitoring suspicious activity

6. Secure API Development

- API authentication (JWT, OAuth basics)
- Rate limiting
- API input validation

7. Secure Coding Standards

- Language-specific best practices (Java/Python/JS)
- Code review checklist
- Secure design patterns

TARGET AUDIENCE: Working professionals, middle-to-senior managers, and business leaders.

COMMERCIAL DETAILS:

Cost: INR 1,20,000/ per participant (for 4 day on campus residential program) excluding GST for a batch of 25 participants.

Note: On successful completion of the program, the participants will be awarded a Certificate of participation from the Institute.

MDP Office Contact Details

<p>Dr. Shailja Agarwal Professor, Business Communications Chairperson: Management Development Programs Ph.: 0120-4083260 mdp@imt.edu , sagarwal@imt.edu</p>	<p>Dr. Amit Sareen Dean Corporate Relations Ph: 0120-4083310 / Ph + 91 9711083075 mdp@imt.edu; amit.sareen@imt.edu</p>
---	---