Customized course related to Java Security

1.Introduction to Java Security

1.1 Overview of Java Security
1.2 Importance of Security in Java Applications

2. Java Security Architecture

2.1 Java Security Model
2.2 Classloaders and Code Sandboxing
2.3 Security Managers

3. Authentication and Authorization

3.1 User Authentication in Java
3.2 Authorization Models
3.3 Role-Based Access Control (RBAC) in Java

4. Cryptography in Java

4.1 Introduction to Cryptography
4.2 Java Cryptography Architecture (JCA)
4.3 Secure Random Number Generation
4.4 Using Java Cryptography Extensions (JCE)

5. Secure Communication

5.1 Overview of Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

5.2 Implementing HTTPS in Java

5.3 Certificate Management in Java

6. Input Validation and Sanitization

6.1 Importance of Input Validation

6.2 Java Validation Libraries

6.3 Protecting Against SQL Injection and Cross-Site Scripting (XSS)

7. Secure Coding Best Practices

7.1 Principle of Least Privilege

7.2 Secure Coding Guidelines

7.3 Code Reviews and Static Analysis Tools

8. Logging and Auditing

8.1 Importance of Logging in Security

8.2 Java Logging Frameworks

8.3 Auditing Security Events

9. Security Testing in Java

9.1 Types of Security Testing
9.2 Using Security Testing Tools
9.3 Integrating Security Testing into the Development Lifecycle

10. Java Security in Web Applications

10.1 Securing Java EE Applications
10.2 Cross-Site Request Forgery (CSRF) Protection
10.3 Session Management Best Practices

11. Secure Deployment

11.1 Securing Java Deployment Environments
11.2 Container Security
11.3 Continuous Monitoring and Incident Response

12. Case Studies and Examples

12.1 Real-world Examples of Java Security Issues
12.2 Lessons Learned and Best Practices