



JAVA TRAINING

Java Security Course

Secure Java applications effectively. Learn to identify and mitigate common Java security vulnerabilities.

DURATION

2 hours

LEVEL

Intermediate

FORMAT

Instructor-Led

-
- Globally Recognized Certification
 - Expert-Led Hands-On Training
 - Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

COURSE OVERVIEW

Unlock the critical skills needed to build robust and impenetrable Java applications with Computer Pride's Intermediate Java Security Course. In today's interconnected digital landscape, securing software is paramount, and Java's widespread use across enterprise systems makes it a prime target for security vulnerabilities. This intensive 2-hour course is meticulously designed to equip intermediate Java developers with the knowledge and practical expertise to identify, prevent, and mitigate common security threats, ensuring the integrity and confidentiality of their applications.

This course dives deep into the core technologies that underpin Java's security architecture, including the Java Cryptography Architecture (JCA), Java Authentication and Authorization Service (JAAS), and the Java Secure Socket Extension (JSSE). You will learn secure coding best practices, understand the OWASP Top 10 vulnerabilities in a Java context, and gain hands-on experience implementing cryptographic services, secure communication protocols, and robust authentication/authorization mechanisms. By mastering these concepts, you'll not only enhance your technical prowess but also significantly boost your value to employers seeking developers capable of building secure, trustworthy software solutions.

Duration	2 hours
Level	Intermediate
Vendor	Java

COURSE CURRICULUM

01 Module 1: Fundamentals of Java Security

- Introduction to Java Security Architecture
- Understanding Java Class Loaders and Security Managers
- Permissions, Policies, and Grants
- Overview of Common Java Vulnerabilities

02 Module 2: Cryptography with Java (JCA & JCE)

- Java Cryptography Architecture (JCA) Basics
- Implementing Symmetric and Asymmetric Encryption
- Hashing and Digital Signatures with JCE
- Key Management and Secure Key Storage

03 Module 3: Authentication and Authorization (JAAS)

- Introduction to Java Authentication and Authorization Service (JAAS)
- Developing and Integrating Login Modules
- Implementing Role-Based Access Control (RBAC)
- Secure Session Management

04 Module 4: Secure Communication (JSSE)

- Java Secure Socket Extension (JSSE) Fundamentals
- Implementing SSL/TLS for Secure Network Communication
- Managing Keystores and Truststores
- Secure Client-Server Communication Patterns

05 Module 5: Secure Coding Practices & Vulnerability Mitigation

- OWASP Top 10 for Java Applications
- Input Validation and Output Encoding Techniques
- Preventing SQL Injection, XSS, and CSRF in Java
- Secure Error Handling and Logging Practices

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

- > **Security-Focused Java Developer**
- > **Application Security Engineer (Java Ecosystem)**
- > **DevSecOps Specialist (Java Backend)**

FREQUENTLY ASKED QUESTIONS

Q: What specific Java security APIs will I master in this course, and how will that enhance my ability to build secure applications?

This course provides in-depth training on critical Java security APIs including the Java Cryptography Architecture (JCA) for encryption and hashing, the Java Authentication and Authorization Service (JAAS) for managing user identities and permissions, and the Java Secure Socket Extension (JSSE) for secure network communications. Mastering these APIs will enable you to confidently implement robust security features, from data protection to secure user access, directly into your Java applications, making them resilient against common attack vectors.

Q: Is this Java Security Course suitable for someone transitioning from general Java development to a security-focused role, and what are the prerequisites?

Absolutely. This intermediate-level course is ideal for experienced Java developers looking to specialize in application security. It assumes a solid understanding of core Java programming concepts, including object-oriented programming, data structures, and basic network programming. While prior security knowledge is beneficial, it's not strictly required, as the course builds foundational security principles specific to the Java ecosystem.

Q: Beyond theoretical knowledge, what practical secure coding skills will I gain to immediately apply in real-world Java projects?

You will gain practical, hands-on skills in identifying and mitigating common Java vulnerabilities such by applying secure coding patterns for input validation, output encoding, and proper error handling. You'll learn to implement secure authentication and authorization flows, manage cryptographic keys, and establish secure communication channels. This practical exposure will enable you to immediately integrate robust security measures into your ongoing and future Java development projects, significantly reducing their attack surface.

ABOUT COMPUTER PRIDE

East Africa's Premier IT Training Center



With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

15+

Years of Excellence

10,000+

Professionals Trained

50+

Vendor Certifications

READY TO ENROL?

Take the next step in your technology career.

Location

1st Flr, ICEA Building
Kenyatta Ave, Nairobi

Email

info@computer-pride.co.ke

Phone

+254 705 900 900

www.computer-pride.co.ke