IT Professional Training Center

Developing Secure Java Code

About the course:

This Developing Secure Java Code course is designed for people involved in the production of Java software applications, and will give delegates useful tools and techniques to harden systems against attack.

It's all too often the case that security comes as an afterthought - if it comes at all, in the drive to keep pushing out new iterations and products. Without being given adequate time to explore security in depth, it's unlikely many development team members will have considered the extent to which businesses are exposed to external - and internal - malicious actors.

Developing Secure Java Code course will give you the techniques and hands-on experience with relevant security tools to help protect your business systems from attackers, and help instill a security-first mindset. We also encourage ways to implement security quickly, efficiently, at the right time, and most importantly, effectively too!

This training uses hands-on technical examples, security tools and teamwork to thoroughly analyze and understand the modern security environment.

We will give delegates access to deliberately vulnerable virtual environments which reflect real-world scenarios in order to learn how to fortify against malicious intrusion.

Our Developing Secure Java Code course also takes a good hard look at the Open Web Application Security Project (OWASP) Top Ten most critical web application security risks and how to guard against them. The following subjects will be covered:

- Know the Secure Design Principles
- Understand OWASP Top 10 attacks
- Understand the Authentication and Authorization problems
- Know how to prevent Cross-Site Scripting
- Know how to prevent Cross-Site Request Forgery
- Understand the secure Development Cycle
- Know how to prevent Injection Attacks
- Understand the protections in JDBC and JPA
- Understand the Penetration Testing methodologies
- Know how to secure Java Applications

Duration:

25 hours (online)

IT Professional Training Center

Prerequisites:

- Experience with Java.
- Experience of creating web applications.

Course syllabus:

- OWASP Top 10 – Hands On
- Secure Development Cycle
- Code Injection
- Final Classes and Methods
- Singletons, Factories, and Flyweights
- Methods, Collections, and Data Hiding
- Sealing JARs
- Code Obfuscation
- Object Serialization
- SQL Injection
- Cross-Site Scripting
    - Reflected XSS
    - Defeating XSS
- CSRF Protection
- Session Management Vulnerabilities:
    - Session Fixation and Hijacking Attacks Protection
    - Session Token
- Logging and Auditing
- Encryption and Digital Signature
- Java Base64 Encoding and Decoding
- Java Secure Hashing
- KeyStores
- Keys and Certificates
- Certificate Authorities
- The KeyStore API
- Signing JARs
- OVal validation framework
- Secure Token Management: JWT, JWE, JWS
- Brief introduction to Java-Based Security Frameworks and Tools:
    - Java EE Security API
    - Apache Shiro
    - Spring Security
    - SonarQube(Continuous Inspection of Code Quality Tool)