Securing JEE Web Services | Secure JEE Web Services Development (TT8500-J)

Modality: Virtual Classroom

Duration: 4 Days

About this course:

Securing the Services of Java Web is a hands-on, lab-intensive JEE course of security training, basic for experienced designers who need to deliver secure JEE-based web administrations. Notwithstanding showing fundamental programming abilities, this course delves profoundly into sound practices and procedures that apply to the whole programming improvement lifecycle.

Designing, deploying, and implementing secure administrations presents unique difficulties. Notwithstanding managing the entirety of the vulnerabilities and assaults related to web applications, web administrations must address business-arranged concerns, for example, authorization, authentication, non-repudiation, and others. The muddling factor is that all estimates must be actualized inside the imperatives of benchmarks and elevated levels of interoperability.

With this course, learners look at best practices for protectively coding the services of JEE, comprising XML processing. Understudies will over and again assault and afterward protect different resources related to completely practical web administrations. This approach of hands-on drives homes the mechanics of how to protect web services of JEE in the most experience of terms.

Security specialists concur that the least viable way to deal with security is "penetrate and patch ". It is unmistakably increasingly viable to "bake" security into an app all through its lifecycle. In the wake of investing noteworthy energy attempting to shield an inadequately structured (from a security viewpoint) web application, designers are prepared to figure out how to create secure web applications beginning at task initiation. The last bit of this course expands on the formerly learned mechanics for building protections by investigating how plan and examination can be utilized to develop more grounded applications from the earliest starting point of the product lifecycle.

The normal pay of a Java engineer is $69,722 every year.

Course Objective:

Understudies who go to Securing Services of Java Web will leave the course equipped with the aptitudes required to perceive genuine and potential programming vulnerabilities, actualize guards for those vulnerabilities, and test those protections for adequacy.

This course rapidly acquaints designers with the most widely recognized security vulnerabilities looked by web applications today. Every defenselessness is inspected from a Java/JEE viewpoint through a procedure of portraying the danger and assault components, perceiving related vulnerabilities, and, at long last, planning, implementing, and testing powerful barriers. Various reasonable labs strengthen these ideas with genuine vulnerabilities and assaults. Understudies are then tested to plan and actualize the layered resistances they will require in protecting their own

applications.

Working in a hands-on, lab-intensive programming condition, driven by our security specialists, guided by our master security group, understudies will figure out how to:

- Have the option to test web applications with different assault strategies to decide the presence of and adequacy of layered resistances.
- Prevent and guard the numerous potential vulnerabilities related to untrusted information
- Comprehend the essentials of XML Digital Signature and also how it may be utilized as a major aspect of the guarded framework for web administrations.
- Comprehend the terminology and concepts behind designing, supporting, and deploying secure services.
- Like the magnitude of the issues related to the security of the services and the potential dangers related to those issues.
- Comprehend the consequences for not appropriately dealing with untrusted information, for example, cross-site scripting, denial of service, and injections.
- Comprehend the presently acknowledged accepted procedures for supporting the numerous security needs of administrations.
- Have the option to identify, assault, and implement protections for authorization and authentication usefulness.
- Comprehend the mechanisms and dangers behind Injection and Cross-Site Scripting (XSS) assaults
- Have the option to identify, assault, and actualize protections against Injection and XSS assaults
- Comprehend the vulnerabilities related to authorization and authentication inside the setting of web administrations.
- Comprehend the terminology and concepts behind protective, secure, coding.
- Comprehend the utilization of Threat Modeling as an apparatus in software vulnerabilities identification dependent on sensible dangers against important resources.
- Perform both reviews of static code and testing of the dynamic application to reveal vulnerabilities in Java-based web administrations.
- Plan and create solid authorization and authentication executions inside the setting of JEE.
- Comprehend the basics of XML Encryption and also how it utilized as an aspect of the cautious framework for web administrations.
- Comprehend and shield vulnerabilities that are explicit to XML and XML parsers.

Audience:

This course of JEE/web services programming intended for engineers who wish to find a good pace on growing admirably shielded applications of the software. This course might be modified to suit your group's unique goals.

Prerequisite:

Understanding with JEE and Java is required and certifiable programming experience is enthusiastically suggested. Understudies ought to have a half year to a time of Java and JEE working information.

Course Outline:

Module 1: Foundation

Lesson: Who is Safe?

- Assumptions We Make
- Security: The Complete Picture
- Anthem, Sony, Target, Heartland, and TJX Debriefs
- Verizon’s 2017 Data Breach Report
- Attack Patterns and Recommendations
- Tutorial: Working with Eclipse (JEE Version) and Tomcat
- Tutorial: Working with the HSQL Database
- Exercise: Case Study Setup and Review

Lesson: Security Concepts

- Motivations: Costs and Standards
- Open Web Application Security Project
- Web Application Security Consortium
- CERT Secure Coding Standards
- Microsoft SDL
- Assets and Trust Boundaries
- Threat Modeling
- Exercise: Case Study Asset Analysis

Lesson: Principles of Information Security

- Security Is a Lifecycle Issue
- Minimize Attack Surface Area
- Layers of Defense: Tenacious D
- Compartmentalize
- Consider All Application States
- Do NOT Trust the Untrusted

Module 2: Applying Security to Services

Lesson: Service Challenges

- Services Overview
- Identity and Propagation
- Real-time Transactions
- Diverse Environments
- Information Protection
- Standards compliance

Lesson: Services and Security

- Security Policies
- Applicable OASIS Standards
- SAML
- SAML Usage Scenarios
- Oauth 2.0 and OpenID
- Exercise: Working with OAuth

Module 3: Defending XML Processing

Lesson: Defending XML

- XML Signature
- XML Encryption
- XML Attacks: Structure
- XML Attacks: Injection
- Safe XML Processing
- Exercise: Safe XML Processing
- Exercise: Dynamic Loading Using XSLT

Lesson: Defending Web Services

- Web Service Security Exposures
- When Transport-Level Alone is NOT Enough
- Message-Level Security
- WS-Security Roadmap
- XWSS Provides Many Functions
- Web Service Attacks
- Web Service Appliance/Gateways
- Exercise: Web Service Attacks

Lesson: Defending Rich Interfaces and REST

- How Attackers See Rich Interfaces
- Attack Surface Changes When Moving to Rich Interfaces
- Bridging and its Potential Problems
- Three Basic Tenets for Safe Rich Interfaces
- OWASP REST Security Recommendations

Module 4: Vulnerabilities (Part 1)

Lesson: Unvalidated Input

- Buffer Overflows
- Integer Arithmetic Vulnerabilities
- Unvalidated Input: From the Web
- Defending Trust Boundaries

- Whitelisting vs Blacklisting
- Exercise: Defending Trust Boundaries
- Exercise: Defending Trust Boundaries With Regular Expressions

Lesson: Broken Access Control

- Access Control Issues
- Excessive Privileges
- Insufficient Flow Control
- Unprotected URL/Resource Access
- Examples of Shabby Access Control
- Sessions and Session Management

Lesson: Broken Authentication

- Broken Quality/DoS
- Authentication Data
- Username/Password Protection
- Exploits Magnify Importance
- Handling Passwords on Server Side
- Single Sign-on (SSO)
- Exercise: Defending Authentication

Lesson: Cross Site Scripting (XSS)

- XSS Patterns
- Persistent XSS
- Reflective XSS
- Best Practices for Untrusted Data

Lesson: Injection

- Injection Flaws
- SQL Injection Attacks Evolve
- Drill Down on Stored Procedures
- Other Forms of Injection
- Minimizing Injection Flaws
- Exercise: Defending Against SQL Injection

Module 5: Vulnerabilities (Part 2)

Lesson: Error Handling and Information Leakage

- Fingerprinting a Web Site
- Error-Handling Issues
- Logging In Support of Forensics
- Solving DLP Challenges

Lesson: Insecure Data Handling

- Protecting Data Can Mitigate Impact
- In-Memory Data Handling
- Secure Pipes
- Failures in TLS/SSL Framework
- Exercise: Defending Sensitive Data

Lesson: Insecure Configuration Management

- System Hardening: IA Mitigation
- Application Whitelisting
- Least Privileges
- Anti-Exploitation
- Secure Baseline

Lesson: Direct Object Access

- Remote File Inclusion
- Redirects and Forwards
- Direct Object References

Lesson: Spoofing, CSRF, and Redirects

- Name Resolution Vulnerabilities
- Fake Certs and Mobile Apps
- Targeted Spoofing Attacks
- Cross Site Request Forgeries (CSRF)
- CSRF Defenses

Module 6: Best Practices

Lesson: Cryptography Overview

- Strong Encryption
- Message Digests
- Encryption/Decryption
- Keys and Key Management
- NIST Recommendations

Lesson: Understanding What's Important

- Common Vulnerabilities and Exposures
- OWASP 2017 Top Ten
- CWE/SANS Top 25 Most Dangerous SW Errors
- Monster Mitigations
- Strength Training: Project Teams/Developers

- Strength Training: IT Organizations

Module 7: Secure Development Lifecycle (SDL)

Lesson: SDL Process Overview

- Types of Security Controls
- Phases of Typical Data-Oriented Attack
- Phases: Offensive Actions and Defensive Controls
- Security Lifecycle Activities

Module 8: Security Testing

Lesson: Testing Tools and Processes

- Security Testing Principles
- Dynamic Analyzers
- Static Code Analyzers
- Criteria for Selecting Static Analyzers

Lesson: Testing Practices

- OWASP Web App Penetration Testing
- Authentication Testing
- Session Management Testing
- Data Validation Testing
- Denial of Service Testing
- Web Services Testing
- Ajax Testing