Web Application Security Workshop (3 Day)

Course Summary

Description

A three-day workshop introducing Java developers to Web Application threat discovery, mitigation, and modeling. This course used OWASP Top 10 as a core focus.

Topics

- Threat Discovery
- Threat Mitigation
- Technology Centric Security and Threat Modeling

Audience

The target audience is Java Backend developers with some knowledge of Java Script Front End Development.

Prerequisites

Before taking this course, students should have knowledge and experience with Java and JEE development including JSP, Spring MVC, Microservice Development and/or Web Service development in SOAP and/or REST; Understanding of JavaScript, NoSql Db and React.

Duration

Three days

Web Application Security Workshop (3 Day)

Course Outline

I. Threat Discovery

Identifying and Discovering threats in Legacy JEE Web Apps, Web Services and Microservices (via hands on labs + using ZAP)

A. Injection
B. Broken Authentication
C. Sensitive Data Exposure
D. XML External Entities
E. Broken Access Control
F. Cross Site Scripting
G. Insecure Deserialization
H. Insufficient Logging and Monitoring
I. Rx Java and potential thread issues

II. Threat Mitigation

Coding workshops and discussions for mitigating Legacy JEE Web Apps, Web Services and Microservices threats

A. Injection
B. Broken Authentication
C. Sensitive Data Exposure
D. XML External Entities
E. Broken Access Control
F. Cross Site Scripting
G. Insecure Deserialization
H. Insufficient Logging and Monitoring

III. Technology Centric Security and Threat Modeling

A. Technology Centric Security
    1. Front End Java Script Security Threats Workshop
    2. Blockchain
    3. React Redux Discussions and Workshop
    4. Coding discussions and optional workshops for mitigating No-SQL Database threats
    5. Security based JUNIT Testing
B. Threat Modeling
    1. Threat Modeling Overview
    2. Threat Model Example
    3. Threat Modeling Workshop