Applications Security Foundations

Course Title: Applications Security Foundations

Duration: 2 days, 16 Hrs

Class Format Options:

Instructor-Led Training/ Classroom

Who Should Attend:

Developers looking to extend their knowledge in Applications Security.

Prerequisites:

- Knowledge of a Programming language (JAVA,
- .NET, PHP).
- Knowledge of Web technology.
- Knowledge of Database Management Systems. (Oracle, MySQL, MSSQL)

Type of Certificate Obtained:

Applications Security Foundations

Course Overview

This course covers the Applications Security Foundations topics that are relevant to a large number of web application developers. In this course you will watch demos of real word attacks and how to prevent them, and gain confidence in the journey to improving the security of your applications.

Teach students concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw, and implementing a fix for that flaw. Learn practical techniques that you can use to prevent common attacks.

Upon Completion

Students will get knowledge in:

- Web Application Security.
- Common Web Application Risks.
- Demo Web Application Penetration
- Data Validation
- Authentication.
- Session Management.
- Secure SDLC.

Course Content

Module 1: Introduction to Software Security

- Course overview.
- Course objectives.
- Introduction.
- Why care about software security.
- Application threats.
- Common vulnerabilities.
- Definitions of software security.
- Secure coding fundamentals.

Module 2: Common Web Application Risks (OWASP Top 10)

- A1 - Injection.
  a) SQL Injection.
  b) OS/Command Injection.
  c) LDAP Injection.
- A2 - Broken Authentication and Session Management.
  d) A3 - Cross-Site Scripting (XSS).
  e) A4 - Insecure Direct Object References.
  f) A5 - Security Misconfiguration.
  g) A6 - Sensitive Data Exposure.
  h) Data at Rest.
  i) Data in Transit.
  j) A7 - Missing Function Level Access Control.

Module 3: Demo Web Application Penetration

- Videos.
- Vulnerability penetration demo.

Module 4: Data Validation

- Input validation.
- Server vs. Client side validation.
- Whitelisting vs. blacklisting
- Output encoding and escaping
- Parameterized queries
- Using frameworks and APIs
- Microsoft Web Protection Library
- Java Regex.
- OWASP ESAPI validators.

Module 5: Authentication

- Basic vs. forms based Authentication.
- Authentication Policies.
- Authorization and permissions.

Module 6: Session Management

- Protecting session IDs.
- Session Hijacking.
- Session Fixation.

Module 7: Secure SDLC

- Overview.
- Secure software development lifecycle.
- A Secure Process.
- Manager's point of view.
- Developer's point of view.
- Consumer expectations.
- Business responsibility.
- Phases of development lifecycle.