education overview

application security education - 2012

instructor led training

Appsecure

strategy. education. research.

The Appsecure Edge.....

We bring an uncommon set of perspectives to our education programs as we understand how developers build technology, how organisations use it and how attackers attack it. This knowledge allows our education programs to be tailored to the specific needs of your company.

- The depth and breadth of our security knowledge and experience is unmatched among training companies. Security is not a one-size-fits all and we are uniquely positioned to understand what security means to your organization.

- We speak the language—a few in fact! Development, IT, security, lines of business—they all speak a different language and come to security with different perspectives, biases and (sometimes) misconceptions. We are fluent in the language—and the culture— of each of these groups, making us ideal translators in organisation wide conversations about security and education within your company.

- We are adaptive, flexible and client focused. Our modular curriculum offers flexibility and we know how to get education programs up and running quickly.

- The Appsecure team has provided education for hundreds of organisations and thousands of developers, qa testers and business managers. Not only do we invest in quality training programs, we assist organisations in implementing short to long term education strategies.

Looking for CBT (Computer based training), Appsecure offers a number of CBT based education programs available online. For more information please talk with your account manager on the options available.

instructor led education

A number of studies have proven that the identification and remediation of vulnerabilities in early stages the software development lifecycle, substantially and cost-effectively reduces information risk. Only recently have companies begun to implement secure software development lifecycle (S-SDL) i.e. integrate security into the software development lifecycle. Application security trainings based on formal software security assurance methodologies play an important role in success of such S-SDLC programmes. We at Appsecure understand this and hence we have created role-specific training for all development staff — whether they are architects, developers, QA testers or managers.

Our courses for development teams begin with an overview of application security concepts. Students not only learn the many ways in which vulnerabilities in software code may be exploited by attackers but are also shown the value of secure coding through hands on labs and code samples. Building on this understanding of the risks inherent in software development, students learn solid architecture designing, testing and implementation principles. From there, they explore the ways to root out security issues within existing systems and how to effectively respond to evolving security threats.

INSTRUCTOR LED TRAINING - COURSES AVAILABLE

DEVELOPMENT STAFF

Coding Secure Applications using Microsoft .NET - 2 Day Course
Coding Secure Applications using Microsoft .NET - 1 Day Course

Coding Secure Applications using Java EE - 2 Day Course
Coding Secure Applications using Java EE - 1 Day Course

QUALITY ASSURANCE STAFF

Application Security for QA/Testing Teams - 2 Day Course
Application Security for QA/Testing Teams - 1 Day Course

GENERAL STAFF

Application Security Fundamentals for Managers - 1 Day Course

The most successful security education programs are role-specific and customized for each organisation's internal policies and development methodologies. Appsecure interviews internal security team and development staff to understand development team policies, controls, and methodologies. One to two weeks of customisation will result in customised role-specific courses designed for application developers, project managers, architects and quality assurance testers.

This course equips the entire development team to reduce information risk by deeply integrating security into the development life cycle. Topics include internal policies and controls, application security fundamentals, secure coding, architecting secure systems, and testing for security.

instructor led courses

(ILT-DS-NET) CODING SECURE APPLICATIONS USING MICROSOFT .NET

Duration: 1 or 2 day course

This role-specific course is designed for developers and architects working in a Microsoft.NET environment. This focused course equips students with a clear understanding of the built-in security features of .NET as well as best practices for coding securely. Topics will include: principles of secure application design, building security controls, common vulnerabilities and mitigation techniques; building secure web services and introduction to secure development processes.

(ILT-DS-JAVA) CODING SECURE APPLICATIONS USING JAVA EE

Duration: 1 or 2 day course

This role-specific course is designed for developers and architects who work in JAVA EE environments. This focused course equips students with a clear understanding of the built-in security features of Java EE as well as best practices for coding securely. Topics include Web application insecurities, principles of secure application design, building security controls, common vulnerabilities and mitigation techniques; building secure web services and introduction to secure development processes.

(ILT-QA-ASSURE) APPLICATION SECURITY FOR QA TEAMS

Duration: 1 or 2 day course

This introductory course is designed for quality assurance professionals who need to understand how to test their systems for common security weaknesses. The course offers its students a comprehensive introduction to common application vulnerabilities and their exploitation techniques and equips them to test for these vulnerabilities before applications go into production. Through lab-based learning, students identify vulnerabilities in a sample application and learn to take these lessons back to their own applications. Topics will include: the attacker mindset; security testing tools and techniques; mapping the application; error handling and information leakage; authentication flaws; authorizations flaws; common server side attacks and common client side attacks and vulnerabilities.

(ILT-GS-FUNDAMENTAL) APPLICATION SECURITY FUNDAMENTALS FOR MANAGERS

Duration: 1 day course

This foundational course is designed for all staff members who lead or manage the application development projects. This introduction to application security equips the attendees with knowledge required to kick start and manage the development of more secure applications. Topics include the OWASP Top Ten, key security principles, setting information security goals and controls, common vulnerabilities and countermeasures, and foreseeing, calculating and managing risk and security in the SDLC.

coding secure applications using microsoft .net

In this course, the attendees will gain in-depth knowledge of the security features in the .Net platform and best practices to design and develop secure and dependable systems.
The course is divided into eight modules as described below:

Module 1 - Application security and secure coding - what and why?

Objective: This is an introductory module which will provide the attendees with an understanding of the application security concepts. It will also help to understand the need and importance of secure software in today's world.

- Introduction to application security
- Application security and need for secure software?
- Different approaches to implement information security
- Resources and Open Source Initiatives
- OWASP Top Ten

Module 2 - Security Features in Microsoft .Net (two day course only)

Objective: This module gives an insight into the security features that have been built into the Microsoft.Net framework and teaches to leverage these features to secure the applications.

- Common Language Runtime
- Strong and Weak Named Assemblies
- Code Access Security
- Assembly Permissions

Module 3 - Common Vulnerabilities and Remediation Techniques

Objective: In this module, the participants will learn about the common client and server side vulnerabilities, ways to attack them and techniques to thwart such attacks.

- Client side vulnerabilities and corresponding mitigation techniques
  - Cross Site Scripting
  - Cross Site Request Forgery
  - Parameter Manipulation
  - HTTP Repsonse Splitting
- Server side vulnerabilities and corresponding mitigation techniques
  - SQL Injection
  - Command Injection
  - LDAP Injection
  - Remote file inclusion
  - Local file inclusion

Module 4 - Building Security Controls using Microsoft .NET

Objective: This module aims at providing attendees with the approaches to build security controls using the libraries that are built into the Microsoft .Net framework and other secure libraries from trusted sources such as OWASP.

- Authentication and Authorisation
- Auditing and Non Repudation
- Exception Management
- Session Management
- Encryption

Course Details

Audience
Programmers and architects responsible for developing enterprise applications using Microsoft.Net

Duration
One Day (fast-paced course)
Two Days (full course)

Pre-requisties
- Understanding of Microsoft .NET framework and programming
- Familiarity with web application programming

coding secure applications using microsoft .net

Course Details

Audience

Programmers and architects responsible for developing enterprise applications using Microsoft.Net

Duration

One Day (fast-paced course)
Two Days (full course)

Pre-requisties

- Understanding of Microsoft .NET framework and programming
- Familiarity with web application programming

Module 5 - Securing Microsoft .NET services

Objective: This module introduces the attendees to web services specific attacks and suggests techniques to defend against such attacks.

- Common Vulnerabilities and Attacks on Web Services
- Securing WCF Services
- Securing WIF Services (2 day course only)

Module 6 - Secure Configuration and Deployment (two day course only)

Objective: This module provides attendees the knowledge of various security related configuration settings available within Microsoft.Net framework. They also learn to use the tools offered by Microsoft to test the security of the application.

- Secure Configuration for ASP.NET and IIS
- Using tools available with Microsoft .Net i.e Security Configuration Editor, FxCop CAT.NET
- DLL Signing

Module 7 - Design Principles for Secure Application

Objective: This module covers the security principles that lay the foundation for a secure application architecture and design.

- Principal of Least Privilege
- Defence in Depth
- Complete Mediation
- Data Privacy
- Security vs. Ease of Use

Module 8 - Secure Development Process (two day course only)

Objective: In this module, attendees discover the ways in which security can be integrated into the software development lifecycle being used for their projects. The attendees are also provided with an introduction to threat modelling.

- Secure Development Lifecycle - Introduction
- Threat Modelling - Introduction

coding secure applications using java ee

Course Details

Audience

Programmers and architects responsible for developing enterprise applications using Java.

Duration

One Day (fast-paced course)
Two Days (full course)

Pre-requisties

- Understanding of Java platform and programming
- Familiarity with web application programming

In this course, the attendees will gain in-depth knowledge of the security features in the Java platform and best practices to design and develop secure and dependable systems. The course is divided into eight modules as described below:

Module 1 - Application security and secure coding - what and why?

Objective: This is an introductory module which will provide the attendees with an understanding of the application security concepts. It will also help to understand the need and importance of secure software in today's world.

- Introduction to application security
- Application security and need for secure software?
- Different approaches to implement information security
- Resources and Open Source Initiatives
- OWASP Top Ten

Module 2 - Security Features in Java (two day course only)

Objective: This module gives an insight into the security features that have been built into the Java EE framework and teaches to leverage these features to secure the applications.

- Java Security Model
- Security Manager
- Policy Tool

Module 3 - Common Vulnerabilities and Remediation Techniques

Objective: In this module, the participants will learn about the common client and server side vulnerabilities, ways to attack them and techniques to thwart such attacks.

- Client side vulnerabilities and corresponding mitigation techniques
  - Cross Site Scripting
  - Cross Site Request Forgery
  - Parameter Manipulation
  - HTTP Repsonse Splitting
- Server side vulnerabilities and corresponding mitigation techniques
  - SQL Injection
  - Command Injection
  - LDAP Injection
  - Remote file inclusion
  - Local file inclusion

Module 4 - Building Security Controls using Java

Objective: This module aims at providing attendees with the approaches to build security controls using the libraries that are built into the Java platform and other secure libraries from trusted sources such as OWASP.

- Authentication and Authorisation
- Auditing and Non Repudation
- Exception Management
- Session Management
- Encryption

coding secure applications using java ee

Course Details

Audience

Programmers and architects responsible for developing enterprise applications using Java EE

Duration

One Day (fast-paced course)
Two Days (full course)

Pre-requisties

- Understanding of Java EE platform and programming
- Familiarity with web application programming

Module 5 - Securing Java services

Objective: This module introduces the attendees to web services specific attacks and suggests techniques to defend against such attacks.

- Common vulnerabilities and attacks on web services
- Securing Web Services

Module 6 - Secure Configuration and Deployment (two day course only)

Objective: This module provides attendees the knowledge of various security related configuration settings available within Java platform.

- Secure Configuration for Container
- Creating policies using Policy Tool
- Static Analysis to identify security bugs
- JAR Signing and Verification

Module 7 - Design Principles for Secure Application

Objective: This module covers the security principles that lay the foundation for a secure application architecture and design.

- Principal of Least Privilege
- Defence in Depth
- Complete Mediation
- Data Privacy
- Security vs Ease of use

Module 8 - Secure Development Process (two day course only)

Objective: In this module, attendees discover the ways in which security can be integrated into the software development lifecycle being used for their projects. The attendees are also provided with an introduction to threat modelling.

- Secure Development Lifecycle - Introduction
- Threat Modelling - Introduction

application security for quality assurance teams

Course Details

Audience

Quality assurance teams responsible for ensuring that the applications being deployed into the production environment are free from defects.

Duration

One Day
Two Days

Pre-requisties

- Understanding of web applications testing techniques

In this course, the attendees will gain an in-depth understanding of testing techniques to identify security bugs in the applications. The course is divided into five modules as described below:

Module 1 - Application security and security testing - what and why?

Objective: This is an introductory module which will provide the attendees with an understanding of the application security concepts. It will also help to understand the need and importance of secure software in today's world.

- Introduction to application security
- Application security and need for secure software?
- Different approaches to implement information security
- Resources and Open Source Initiatives
- OWASP Top Ten

Module 2 - Common vulnerabilities and Testing Techniques?

Objective: In this module, attendees learn about the common and dangerous client and server side vulnerabilities and tools and techniques to test the application for presence of these vulnerabilities.

- Tools of the Trade
- Client side vulnerabilities and corresponding mitigation techniques
  - Cross Site Scripting
  - Cross Site Request Forgery
  - Parameter Manipulation
  - HTTP Repsonse Splitting
- Server side vulnerabilities and corresponding mitigation techniques
  - SQL Injection
  - Command Injection
  - LDAP Injection
  - Remote file inclusion
  - Local file inclusion
- Web service specific vulnerabilities and attacks

Module 3 - Testing Security Controls

Objective: In this module, attendees learn techniques to test these controls to ensure the controls are implemented to provide adequate protection.

- Authentication and Authorisation
- Auditing and Non Repudation
- Exception Management
- Session Management
- Encryption

application security for quality assurance teams

Module 4 - Security Testing Processes

Objective: In this module, attendees discuss and discover the ways in which security can be weaved into their software development lifecycle. The attendees also learn the basics of threat modelling and how it can help in testing a system's security.

- Security testing methodology
- Introduction to threat modelling
- Vulnerability scanning using automated tools

Module 5 - Hands-on Application Security Testing

Objective: In this final module, the attendees will be asked to apply the knowledge gained in all previous modules to identify the vulnerabilities present in the given vulnerable application.

- Planning for security testing
- Abuse case creation
- Vulnerability identification and exploitation

application security fundamentals for managers

In this course, the attendees will gain an understanding of application security concepts and learn to calculate and manage the risk from application security related threats. The course is divided into four modules as described below:

Module 1 - Application Security - What and Why?

Objective: This is an introductory module which will provide the attendees with an understanding of the application security concepts. It will also help to understand the need and importance of secure software in today's world.

- Introduction to application security
- Application security and need for secure software?
- Different approaches to implement information security
- Resources and Open Source Initiatives
- OWASP Top Ten

Module 2 - Drivers for secure applications

Objective: In this module, attendees will learn of key application security drivers and guidelines to assist in assessing the need for application security c ontrols for an application.

- Data Privacy in application security
- Compliance and regulatory requirements
- Risk forecasting

Module 3 - Common Vulnerabilities and their impact

Objective: In this module, attendees learn about the common and dangerous client and server side vulnerabilities and potential impact of these vulnerabilities on the business and application users.

- Client side vulnerabilities and corresponding mitigation techniques
  - Cross Site Scripting
  - Cross Site Request Forgery
  - Parameter Manipulation
  - HTTP Repsonse Splitting
- Server side vulnerabilities and corresponding mitigation techniques
  - SQL Injection
  - Command Injection
  - LDAP Injection
  - Remote file inclusion
  - Local file inclusion

Module 4 - Secure Development Processes

Objective: In this module, attendees discuss and discover the ways in which security can be weaved into their software development lifecycle. The attendees also learn the basics of application risk management.

- Secure development lifecycle – Introduction
- Application risk management using STRIDE / DREAD

Course Details

Audience

Project managers responsible for leading the development and delivery of quality software.

Duration

One Day

Pre-requisties

- Understanding of software development processes and web applications.