education overview

application security education - 2012

lecture series

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.

lecture series

Although we have been preaching for years that no application security programme is complete without methodical training of project members, we also realise that it is a tough task to ask 10-15 key project members to leave everything where it is and confine themselves in a training room for 2 days. Furthermore, in these courses attendees are overwhelmed with the amount of information presented, making it difficult for them to grasp, retain and apply everything that has been discussed in the course.

AppSecure proudly announce its 'first of its kind in Asia Pacific' web application security lecture series. We have broken down our renowned training courses into self-contained highly interactive 2 hour lectures. In every lecture, trainer focuses on a particular topic and use examples and demonstrations to provide just enough information that can be grasped by attendees.

Lecture sessions focus on at specific topics, and are designed to be interactive and interesting to capture the audience's attention. Attendees of each session will gain a rapid but in-depth understanding of the application security topic being presented, whilst also gaining a detailed technical and business knowledge of the risks associated with the topic.

The lecture series available from Appsecure includes the following topics:

- Lecture 1: Information Security - What and Why?
- Lecture 2: An introduction to the OWASP Top 10
- Lecture 3: Client Side Vulnerabilities - Detection and Prevention
- Lecture 4: Server Side Vulnerabilities - Detection and Prevention
- Lecture 5: Web Services Security
- Lecture 6: Principles of Secure Application Design and Architecture
- Lecture 7: Threat Modelling - An Introduction
- Lecture 8: Application Security for Project Leaders
- Lecture 9: Automated security testing techniques - Static Analysis
- Lecture 10: Automated security testing techniques - Dynamic Analysis

Course Details

Audience
Lecture series are designed for a wide range of attendees including programmers, architects, managers and general IT staff.

Duration
Lecture series talks are 1.5 to 2 hours each

Pre-requisties
- Varied depending on course

lecture series

Lecture 1 - Information Security - What and Why? (LCT-1-IS)

Everyone in the organisation involved in application development need to know about information security and the impact of insecure applications on the organisation. In this lecture, the trainer will shed light on the concepts of information security, information security terminology, approaches to tackle information security issues and positioning of application security in organisation's information security paradigm. At very least, the attendees of this lecture will learn:

- What is information security and it's importance to an organisation?
- The information security vocabulary – vulnerability, exploit, attacker, risk etc.
- Different approaches to implement information security in an organisation
- The Case of Application Security
- Resources and Open Source Initiatives

Lecture 2 - An introduction to the OWASP Top 10 (LCT-2-T10)

This introductory lecture from Appsecure aims at educating the development teams about the most important and common web application security weaknesses. The attendees are provided with a very high level overview of these vulnerabilities, their impact and generic techniques to avoid these vulnerabilities. The attendees of this lecture will learn:

- The need for application security
- OWASP Top 10 project
- Top 10 most common vulnerabilities and attacking techniques
- Techniques to protect from these vulnerabilities
- Other similar projects and initiatives

Lecture 3 - Client Side Vulnerabilities - Detection and Prevention (LCT-3-CSV)

Several industry reports show that the client side vulnerabilities are among the most exploited vulnerabilities in today's world and the number is continuously increasing. In this lecture, attendees will learn about the common client side vulnerabilities such as XSS, CSRF, Clickjacking etc. They will also learn practical ways to detect these vulnerabilities in the application and secure coding techniques to avoid these vulnerabilities. The attendees will be able to demonstrate

- The knowledge of various client side attacks
- Techniques to test for client side vulnerabilities
- Secure coding techniques to root-out these vulnerabilities

Lecture 4 - Server Side Vulnerabilities - Detection and Prevention (LCT-4-SSV)

Server side vulnerabilities typically are more dangerous than client side vulnerabilities. Attackers can take advantage of these vulnerabilities to gain unauthorised access to the database, application server and even the underlying infrastructure.
The attendees will be able to demonstrate

- The knowledge of various server side attacks such as SQLi, Command Injection, LDAP Injection, RFI and LFI
- Techniques to test for server side vulnerabilities in the applications
- Secure coding techniques to protect the application from these vulnerabilities

lecture series

Lecture 5 - Web Services Security (LCT-5-WSS)

Web services are not just get affected by vulnerabilities those exist in web applications, but also have their own share of specific ones. In this lecture, we look at the vulnerabilities specific to web services and respective mitigation techniques. The attendees of the lecture will learn:

- Various web service vulnerabilities such as schema poisoning, routing detour, XXI and XML Morphing
- Testing techniques to identify web service level vulnerabilities
- Secure coding techniques to avoid these vulnerabilities
- Web service security standards

Lecture 6 - Principles of Secure Application Design and Architecture (LCT-6-SAD)

Over the years, secure coding advocates have researched and provided a set of principles which if implemented aid in designing and building secure applications. In this lecture, attendees will learn each of these principles and will be shown practical ways of implementing these via real life examples. At very least, the attendees of this lecture will learn to:

- Design secure applications based on principles of secure application design and architecture such as complete mediation, defence in depth, principle of least privilege etc.
- Define data privacy requirements for an applications
- Identify the fine line between security and ease of use

Lecture 7 - Threat Modelling - An introduction (LCT-7-TM)

Threat Modelling is a vital step in the development of secure software systems. It enables the software architects and developers to analyse the software from attacker's perspective and help them to put appropriate controls in place to minimize the risk from real world threats. This lecture will help the participants in gaining a conceptual understanding of threat modelling along with the practical ways to integrate it into their software development life cycle.
The attendees of the lecture will learn to:

- Analyse the target application from an attacker's perspective
- Create attack trees and threat models
- Create abuse test cases based on the threat models

Lecture 8 - Application Security for Project Leaders (LCT-8-SPL)

As much it is needed for development team to learn about application security, it is equally important for leaders or managers of development projects to understand application security risk and the various activities they can use to predict, calculate and track the application security of their project. This lecture from AppSecure introduces its attendees to the application security management world and provides information on tried and tested tools and methodologies to kick start building secure applications.
After the lecture, the attendees will be able to:

- Forecast the risk to the application from external factors
- Define data privacy and compliance needs for the application
- Calculate risk from the vulnerabilities using proven methodologies
- Identify the areas of weakness in the application requiring focus

lecture series

Lecture 9 - Automated security testing techniques - Static Analysis (LCT-9-SSA)
Source code review is the process of analysing the application in source form to identify the security vulnerabilities and ensure that appropriate security controls are present and work as intended by the developers and architects. In large scale code review operations for enterprises such that the volume of code is enormous, automated code review techniques can assist in improving the throughput of the code review process.
Through this lecture, the attendees will learn:

- How static analysis tools work?
- The benefits and limitations of static analysis
- Design a software development lifecycle with Integrated static analysis tools
- Using a static analysis tool to identify security bugs

Lecture 10 - Automated security testing techniques - Dynamic Analysis (LCT-10-SDA)
Security testing a.k.a. Penetration testing is a manual technique to analyse a running application to identify security vulnerabilities. In highly dynamic environments where manual regression security testing is not feasible, specialised tools can be used to automate this process. This form of security analysis is called dynamic analysis.
Through this lecture, the attendees will learn:

- How dynamic analysis tools work?
- The benefits and limitations of dynamic analysis
- Design a software development lifecycle with Integrated static analysis tools
- Using a dynamic analysis tool to identify security bugs in the applications

ABOUT APPSECURE
Appsecure is Asia Pacific's leading application security consulting company, specialised and dedicated to help organisations build and successfully execute application security programs.

Appsecure's team of security consultants and reseachers have a combined experience of over 30 years in the field of application security and development. Most of them have excelled in one or more phases of software development prior to expanding into the security field. This real world experience provides the technical depth and breadth required to deliver the enterprise-grade services to our clients.

Appsecure's enterprise-grade application security services range from penetration tests to end-to-end application security programs. For more information visit our web site, or contact us directly **info@appsecure.com** or **1300 736 778**

www.appsecure.com