Secure Software Development Workshop

Sufyan Almajali
Princess Sumaya University for Technology
Computer Science Department
October 8, 2017

Abstract

Most organizations and software development companies focus their software development efforts on creating, releasing, and maintaining a functional software. However, the increasing concerns and business risks associated with insecure software have brought increased attention to the need to integrate security into the development process during all of the stages of Secure Software Development Life Cycle (SDLC). This workshop presents the industry best practices related to secure software development.

Keywords: Secure Software Development, Threat Modeling, Security Testing

Description

This workshop includes a coverage of the industry best practices for secure software development during analysis, design, coding, testing, and maintenance stages. This workshop covers the security and safety analysis in software design and development. It defines the basic security principles. Topics include threat modeling, defensive programming, web security and database security.. In particular, topics include the following:

- Why You Need To Learn Secure Programming
- Secure Software Development Process
- Principles of Security and Quality
- Software Requirements and Security
- Designing for Security
- Development Tools and Security
- Testing for Quality and Security
- Web Security
- Database Security

Requirements for the participants

To be able to participate in the hands-on sessions during the workshop you will need a PC with the following installed PhP/MySQL using XAMPP, Visual Web Developer and MS SQL, and Oracle VM Virtual box with a kali Linux VM downloaded prior coming to class.

Provided materials

The presentations, software, and labs will be available on the workshop day. A handout of set of summaries, examples, and labs will be provided as well.

Timetable

- **9:00-40:00** Introduction: Secure Software Development Process and Principles of Security
- **9:40-9:55** Analysis: Security Uses Cases
- **9:55-10:20:** Design: Threat Modeling and Security Design Patterns
- **10:20-11:00** Lab and Exercise on Security Use cases and Design
- **11:00-11:15** Coffee Break
- **11:15-12:00** XSS and SQL Injection Attacks
- **12:00-13:00** Hands-on: XSS and SQL Attacks
- **13:00-14:00** Lunch
- **14:00-14:30** Database Security
- **14:30-15:00** Lab on Database Security
- **15:00-15:30** Security during Testing and Maintenance
- **15:30-16:30** Lab and conclusion

Outcomes

By the end of this workshop attendees will be able to:

- Recognize secure programming concepts and principles
- Identify key characteristics of secure code
- Secure against common attacks such as XSS and SQL injection
- Secure databases
- Test and maintain a software for security

About Presenter

Sufyan Almajali is an assistant professor at Princess Sumaya University for Technology. Dr. Almajali obtained his Bachelor's and Master's degrees in Computer Science from the University of Jordan. He obtained his Ph.D. in Computer Science from Illinois Institute of Technology, Chicago, IL. He has 17 years of academic and industrial experience. He taught at Robert Morris University, Devry University, and Benedictine University in the United States in the period between 1999 and 2011, and has been at Princess Sumaya University since 2011. Dr. Almajali's teaching experience covers courses in three main areas, namely Software Development, Computer Networking, and Security. In addition to teaching, Dr. Almajali worked in multiple companies in the United States. He served as a senior network engineer at LucidLine Inc., Patron Systems, Inc., and Cybervault Security companies in Chicago, USA. In addition, Dr. Almajali served as chief technology officer at Secure Data Replicator in Chicago, where he supervised the development of an online real-time data replication system.