Building Security In – Think Like a Hacker

Course Objective

Cybersecurity is one of the major issues that IT industry is facing today. The threat of security breach exists at IT infrastructure perimeter, network, hosting environment, and application levels and its extent is on the rise. Besides, the cybersecurity hackers are constantly on the move to find new ways to invade IT security which makes it difficult for the organizations to maintain its security promise to its customers.

The objective of this course is to understand and learn important elements of a web application security and a development lifecycle that will yield a sound web application with minimal security risk. Using OWASP framework, the course first analyzes the most critical web application security risks with respect to access control, network OSI, encryption, environment, and deployment process. For a typical iteration in an agile development environment, it then lays out security related stories and acceptance criteria thus building a sound software development lifecycle (SDLC). The focus of this course is to provide a thorough understanding of security risks and how they can be overcome by following a well-designed development lifecycle.

Intended Audience

The course is intended for individuals that are responsible for building, deploying, and maintaining a web application that is secure and has minimal security risk. It is ideally suited for software development groups, DevOps, and software quality professionals.

Instructional Methods

The course is offered as a ONE DAY workshop with group discussions and role playing where the participants work in small teams. Each team will be dedicated to explore a unique vulnerability end-to-end thereby, understanding the attack surface, impact, root cause, and the vulnerability proofing in the SDLC to eradicate the vulnerability. The instructor will build a step by step module of security breach and its prevention which each team applies to a type of vulnerability. Each team discusses its thought process for each step and gets review feedback with the other teams. By the end of the workshop, a comprehensive document is produced on each vulnerability.

Course Overview

The course starts with building an appreciation for the security by highlighting prominent breach events occurred in both Govt. and private sector. The participants then select a handful of high risk vulnerabilities known today. The discussion is then focused on the Web Application environment and infrastructure and how a hacker takes advantage of a security hole. The course then takes the participants through a complete analysis of the vulnerability and the measures to include in the SDLC.

Course Outline

1. Security Vulnerabilities including OWASP Top 10
2. Vulnerability Analysis specific to compromised web environment components

3. In-depth understanding of the weaknesses of each of these components
4. Addressing these weaknesses during the SDLC especially
    a. Asset evaluation
    b. Threat Modeling
    c. Design for Security
    d. Coding for security
    e. Testing for security including Penetration testing
5. Security reporting to make a release decision

The end product of the course will be an understanding of the following aspects of a secure product development:

Stakeholders in a Secure Web Application Development – Determining organizational functions that are critical in developing a successful product that will provide an ultimate security.
Establishing Security Activities and acceptance criteria for an Iteration Planning – Identifying significant security related activities in iteration Zero and in a typical iterations along with acceptance criteria.
Evaluation of security status at the end of each iteration – Validating security as a elease requirement to assure that product meets iteration requirements.
Security assessment and reporting prior to release – Evaluation of overall application security and publishing a report.
Customization of Product Lifecycle – Understanding your product development ecosystem and customizing the roadmap for the highest possible return.

Prerequisites:

Basic understanding of web application security and the agile product development methodology.

Keywords: Cyber Security, Web Application Security, AppSec, Software Development, Software Engineering, Product Lifecycle, Software Process Improvement, Software Development Lifecycle

Materials - Course notes containing slide presentation

Course Contents – Detail Description

Web Application Introduction

1. Definitions
2. Need for a Web Application and its Security
3. Execution Mechanism of a Web Application – Network Layer, Operating system
4. Impact on Computing Environment / Resources – Operating system, Database Application
5. Potential Vulnerable Areas

Introduction to Malware and Virus

1. How do malware and viruses work?
2. Damages inflict by a virus/malware
3. Security measures – anti-virus, firewalls etc.

OWASP

1. Introduction to OWASP
2. OWASP Top 10 Vulnerabilities
3. Sources for OWASP top 10
4. Protecting Against OWASP Top 10

Biographical information on instructor:

Bhushan Gupta has 30 years of experience in software engineering, 20 of which have been in the software industry. For the past several years, Bhushan has been involved with agile processes, quality methods and metrics, and general process improvements. Bhushan has been a presenter and a reviewer for PNSQC and has also presented at other conferences. As a change agent, Bhushan volunteers his time and energy for organizations that promote software quality.

Bhushan Gupta has a MS degree in Computer Science from New Mexico Institute of Mining and Technology, Socorro, New Mexico, 1985.

Bhushan Gupta has been actively involved in researching several areas of software engineering and has published several articles on Agile Software Development, Web Application Security, Software Quality – attributes, metrics, and reporting.

List of Publications:

1. Bhushan B. Gupta***,*** *Web Application Security – What You Need to Know****,*** 33rd Pacific Northwest Software Quality Conference, Portland, Oregon, October 2015

2. Bhushan B. Gupta, Challenges of Agile Development with an External Vendor: A Case Study, 31st Pacific Northwest Software Quality Conference, Portland, Oregon, October 2013

3. Bhushan B. Gupta, Waterfall to Agile: Flipping the Switch, 30th Pacific Northwest Software Quality Conference, Portland, Oregon, October 2012

4. Bhushan B. Gupta, Driving Product Quality Towards Release Goals, 28th Pacific Northwest Software Quality Conference, Portland, OR October 2010.

5. Bhushan B. Gupta, Is your Testing Effective and Efficient? 26th Pacific Northwest Software Quality Conference 2008, Portland, Oregon October, 2008

6. Bhushan B. Gupta and Orhan Beckman, Ph. D., Quantifying Software Quality, 24th Pacific Northwest Software Quality Conference 2006, Portland, OR October, 2006

7. Bhushan B. Gupta, Guiding Software Quality by Forecasting Defects Using defect Density, 22nd Pacific Northwest Software Quality Conference, Portland, OR October 11-13, 2004

8. Bhushan B. Gupta and Orhan Beckman, Managing Requirements Across Multiple Related Products, Practical Software Quality Techniques, March, 2004, Washington, DC

9. Orhan Beckman, Bhushan Gupta, and Steve Sheffels, Requirements Elicitation for “Customer Delighting” Product Families, 21st Pacific Northwest Software Quality Conference, October 2003, Portland, Oregon

10. Bhushan B. Gupta, Key Factors in Making Offshore Software Development Successful, Better Software and Expo Conference, Software Quality Engineering, September 2004, San Jose, CA

11. Bhushan Gupta and Binnur Al-Kazily, Shifting Paradigm to Agile Methods – Embracing the Change, 21st Pacific Northwest Software Quality Conference, October 2003, Portland, Oregon

12. Bhushan B. Gupta and Steve Rhodes, Adopting a Lifecycle for Developing Web Based Applications, 14th International Software Quality Week, May 2001, San Francisco, CA

13. Bhushan B. Gupta and Steve Rhodes, EVO - A Lifecycle for Developing Web-Based Applications at Internet Speed, Seventh International Conference on Practical Software Quality Techniques, March 2001, Orlando, Florida

14. Bhushan B. Gupta, Defect Causal Analysis – A Grass Root Approach, International Conference on Practical Software Quality Techniques, Austin, TX, March 2000,