Secure Software Development Life Cycle [Web Application]
Integrating Security across SDLC Phases

Workshop Scope & Modules

Hack2Secure
INSPIRE • INDUCE • INNOVATE
www.hack2secure.com
Application Security

Challenges

"Maturing" or "Partially Integrated" Security Practices
Inadequate Mapping of Business & Security Requirements
Missing Security Definitions, Policies & Guidelines
High Security Control Implementation Cost
Handling 3rd Party Components & their Vulnerabilities
Lack of Security Awareness & Skills
Rise in Application Security Vulnerabilities

So, what can be done…?
To address these Security Needs

RISK...
- evaluate
- strategy
- process
- analysis

Copyright © 2016 Hack2Secure India Pvt. Ltd. www.hack2secure.com
Hackers are continuously exploring new Tools, Techniques and Measures to attack an application and gain control on it for their malicious purpose. Typically, Security is considered as Developer’s task to implement and Tester’s task to ensure in any application development process. However, their major focus is on Application Functionality and Features and Security is the last preferable item in their list.

This approach has been proved disastrous time and again, as it always leads to last minute unplanned changes to incorporate fix for security flaw or requirement, additional complexity in code or distorted functionality, missed out of number of security compliance requirements and may lead to untested shipped vulnerabilities. Moreover, unexplored threat vectors also adds-up to the woes and may result as major reason behind security attack or compromise.

Secure SDLC is a structural concept to integrate Security at every phase of SDLC. Ensuring security in a product from scratch, not only helps in ensuring all compliances and basic security requirements but can also provide security from Design, Coding and Process prospect.
Secure SDLC: How it helps

- Early Identification & Mitigation of Security Vulnerability
- Reduce Security Control Implementation Cost
- Awareness of Potential Engineering Challenges
- Security Strategies & Tools to Reduce Development Cost
- Facilitation of Informed & Measurable Security Risk Management
- Comprehensive Risk Management
- Ensure Secure and Industry Compliant Software

Relative Cost of Addressing Security at different Stages
Workshop: Secure SDLC - Web Application

Key Features

Aligned with Standards & Best Practices

- NIST SP 800-64, ISO 27034
- PCI DSS, NIST & FIPS Recommended Security Practices
- BSIMM & OpenSAMM Frameworks
- OWASP Web Application Security Testing Guide
- OWASP Secure Coding Practices, Review Guide
- CERT Secure Coding Practices .. & many more

What You will Learn

- Deep-dive into different different phases of SDL from Security prospect
- Learn to integrate Security in different development methodologies like Agile
- Walk through different Security Assurance Methodologies & Risk Management Techniques
- Learn to identify Application Security Requirements and build Checklist accordingly
- Walk through Product Security Policy
- Deep-dive into Threat Modeling process & Secure design Considerations
- Deep-dive on OWASP Top10 Web Application Security Risk
- Secure Coding practices and Manual Review Guidelines
- Application Security Testing Methods, Tools & Techniques
- Building Final Security Review Plan
- Software Supply Chain Risk Management
- Incident Handling Plan
- Security Patch Management
- Application Disposal Policies

Delivery

- Real Time Case Studies and Scenarios
- Interactive Games, Quiz & Lab for Concept building
Workshop: Secure SDLC - Web Application

Who Needs to Attend?

- Management to get insights of different Business Processes involved at Security end
- Application Development Engineers: Architects, Developers & Testers (QA)
- Software Consultants
- Web Application Security: Engineers, Testers and Analyst
- Web Application Penetration Testers, Auditors and Consultants
- Anyone, who wants to deep-dive into Web Security Testing process, Tools & Techniques

Requirement/Pre-Requisites

- Awareness on Software Development Methodologies
- Knowledge of Web Technologies
- Basic Protocol functionality of Protocols especially HTTP
- Basic knowledge of UNIX & WINDOWS Operating System

Must-Have

Students need to bring their Laptop to access Lab environment

Duration

6 Days

Certification*

- Globally Deliverable, Online via Pearson VUE
- 150mins; 90 MCQ based on Scenarios & Case Studies

*Note:
1. Available from Feb. 2017
2. Certification is NOT included as a part of Workshop deliverable
Topics & Scope

Phase#1: Training phase
- About Secure SDLC
- Core & Design Security Concepts
- Security Assurance Methodologies
- OWASP Top10 Web Application Security Risk

Phase#2: Addressing Security Requirements
- Ensuring Security Requirements
- Addressing Web Vulnerabilities in Requirement Phase

Phase#3: Ensuring Secure Design
- Why we Need to Secure Design
- Attack Surface Analysis
- Threat Modeling

Phase#4: Establishing Secure Implementation Process
- Common Web Application Security Coding Errors
- Secure Coding Best Practices
- Security Code Review/Analysis

Phase#5: Application Security Testing / Verification
- Application Security Testing
- WAST Methodology, Tools and Techniques
- Handling Security Defects

Phase#6: Security Review & Response
- Final Security Review Plan
- Auditing, Vulnerability Assessment & Penetration Testing Process
- Incident Handling Plan
- Threats to Supply Chain Software
- Software Supply Chain Risk Management (SCRM)

Phase#7: Security in Maintenance Cycle
- Security Patch Management
- Application Disposal Policy
[Security Training]

Hack2Secure excels in delivering intensive, immersion Security Training programs designed to master practical steps necessary for defending systems against the dangerous security threats. Our wide range of Vendor Independent Customizable Training courses allow individual to master different aspects of Information Security as per their industry requirement and convenience. These theoretical sessions incorporated with real time examples along with unique hands-on lab allows an individual to easily get ready for practice.

[Security Services]

Hack2Secure offers IT Security Professional Services to ensure measures to stay ahead of Security Threats through adaptive and proactive Security methods
- Secure SDLC Process Awareness, Implementation & Consultation
- Secure Application Design, Threat Modeling
- Application Security Testing
- Security Risk Management
- Vulnerability Assessment & Penetration Testing