Software Security Testing

Overview

Your organization is doing well with functional, usability, and performance testing. However, you know that software security is a key part of your assurance and compliance strategy for protecting applications and critical data. Left undiscovered, security-related defects can wreak havoc in a system when malicious invaders attack. If you don't know where to start with security testing and don't know what you are looking for, this course is for you. It describes how to get started with security testing, introducing foundational security testing concepts and showing you how to apply those security testing concepts with free and commercial tools and resources. Offering a practical risk-based approach, the instructor discusses why security testing is important, how to use security risk information to improve your test strategy, and how to add security testing into your software development lifecycle.

Course Objectives

At the end of the course, successful trainees will be able to:

- Learn how testing professionals can effectively security test software
- Discover how applications are developed and tested with security in mind
- Learn how to use security requirements to plan your testing efforts
- Explore key aspects of security testing – web security, threat modeling, risk assessment
- Examine technical and team skills you need for success
- Learn to use common security testing tools for a variety of testing purposes

Syllabus

1. **SECURITY TESTING – OVERVIEW**
    - What is Security Testing?
    - Example
2. **SECURITY TESTING – PROCESS**
    - Penetration Test – Workflow
    - Footprinting
    - Footprinting –Steps
    - Scanning
    - Enumeration
    - Exploitation
3. **SECURITY TESTING – MALICIOUS SOFTWARE**
    - Malwares
    - Preventive Measures

- Anti-Malware Software

4. **SECURITY TESTING – HTTP PROTOCOL BASICS**
    - HTTP Protocol
    - Basic Features
    - Architecture
    - HTTP Parameters
    - HTTP Messages
    - HTTP Requests
    - HTTP Responses
    - HTTP Methods
    - HTTP Status Codes
    - HTTP Header Fields
    - Client Request Headers
    - Server Response Headers
    - Entity Headers
    - HTTP Security

5. SECURITY TESTING – HTTPS PROTOCOL BASICS

- When is HTTPS Required?
- Basic Working of HTTPS

6. SECURITY TESTING – ENCODING AND DECODING

- What is Encoding and Decoding?

7. SECURITY TESTING – CRYPTOGRAPHY

- What is Cryptography?
- How Encryption Works?
- Cryptography Techniques

8. SECURITY TESTING – SAME ORIGIN POLICY

- What is Same Origin Policy?
- Example
- Same Origin policy Exceptions for IE

9. SECURITY TESTING – TESTING COOKIES

- What is a Cookie?
- Properties of Cookies
- Cookie Contents
- Types of Cookies
- Testing Cookies

- Viewing and Editing Cookies

10. SECURITY TESTING – HACKING WEB APPLICATIONS

- Web Application - PenTesting Methodologies
- OWASP Top 10
- Application - Hands On
- Web Proxy
- Configuring Burp Suite

11. SECURITY TESTING – TESTING INJECTION

- Web Application – Injection
- Examples
- Preventing SQL Injection

12. SECURITY TESTING – TESTING BROKEN AUTHENTICATION

- Preventing Mechanisms

13. SECURITY TESTING – TESING CROSS-SITE SCRIPTING

- Types of XSS
- Example
- Preventive Mechanisms

14. SECURITY TESTING – INSECURE DIRECT OBJECT REFERENCES

- Example
- Preventive Mechanisms

15. SECURITY TESTING – SECURITY MISCONFIGURATION

- Example
- Preventive Mechanisms.

16. SECURITY TESTING – TESTING SENSITIVE DATA EXPOSURE

- Example
- Preventive Mechanisms

17. SECURITY TESTING – MISSING FUNCTION LEVEL ACCESS CONTROL

- Example
- Preventive Mechanisms

18. SECURITY TESTING – CROSS-SITE REQUEST FORGERY (CSRF)

- Example
- Preventive Mechanisms

19. SECURITY TESTING – COMPONENTS WITH VULNERABILITIES

- Example
- Preventive Mechanisms

20. SECURITY TESTING – UNVALIDATED REDIRECTS AND FORWARDS

- Example
- Preventive Mechanisms

21. SECURITY TESTING – AJAX SECURITY

- Example
- Preventive Mechanisms

22. SECURITY TESTING – WEB SERVICE SECURITY

- Preventive Mechanisms

23. SECURITY TESTING – TESTING BUFFER OVERFLOWS

- Example
- Preventive Mechanisms

24. SECURITY TESTING – TESTING DENIAL OF SERVICE

- Symptoms of DoS
- Preventive Mechanisms

25. SECURITY TESTING – MALICIOUS FILE EXECUTION

- Example
- Preventive Mechanisms

26. SECURITY TESTING – AUTOMATION TOOLS

- Open Source Tools
- Sets Commercial Black Box Testing tools
- Free Source Code Analyzers
- Commercial Source Code Analyzers

Audience

This course is appropriate for software development and testing professionals who want to begin doing security testing as part of their assurance activities.

Duration

- (3) Days
- (24) Hours: (8) Hours/Day.

Pre-requisite:

A background of basic software testing principles is required.