HT102 - Application Vulnerability Assessment

This course is designed to train participants to perform threat and vulnerability assessment, understanding the fundamental technical skills required to identify and prevent **application vulnerabilities**. You will also discuss about **methods to support secure software development**. This course is useful for security personnel and others who may be responsible for assessing and **managing the risk of threats to process** facilities.

**Course Agenda:**

**DAY 01**

- **Module introduction**
  - Overview of the first day

- **Application Fundamentals**
  - What is an application?
  - Application taxonomy
    - Client-server model
    - Fat client, thin client, etc.

- **Web Application Fundamentals**
  - What is a web application?
  - Modern web architecture (multi-tiered architecture)
    - Web ecosystem terminology
      - Web server, app server, web service, etc..
  - Web technologies
    - Client-side technologies
      - e.g., Java Applet, Web Start, ActiveX, JavaScript, etc..
    - Server-side technologies
      - e.g., Ruby on Rails, PHP, Java, ASP.NET, etc..
  - Web app development pattern: the MVC
  - Web App VS Application Framework VS Infrastructure
  - Application Protocols and Integration
    - Application VS transport protocols
    - Introducing the HTTP protocol
      - Basics (request, responses, etc.)
    - **LAB - Intercepting browser HTTP traffic**
      - Introducing Burp Suite Proxy
      - Configure the browser in order to intercept traffic
      - Intercepting and replying HTTP traffic with Burp Suite
• HTTPS Basics (SSL, TLS, handshake, certificates, etc.)
  • LAB - Intercepting HTTPS traffic with Burp Suite
    ○ Temporary installation of custom certificates
    ○ Exporting and installing Burp’s custom certificate
  ○ Sessions and Cookies
    • LAB - Analysis of cookies delivery
  ○ Same Origin Policy
    • LAB - Analysis of a cross-domain communication with JavaScript
  ○ Encoding Basics
    • What encoding is?
    • Encoding VS Encryption
    • Common type of encoding: ASCII, Unicode, URL Encoding, etc.
    • LAB - Identify and decode common types of encoding
• LAB - Overview of Burp Suite tools

DAY 02

• Recap of the previous day
• Module introduction
  ○ Overview of the first day
• Application VA Methodology
  ○ Vulnerability Assessment Methodology standards
  ○ Overview of the proposed VA Methodology
• Step 1+2 - Planning and Information Gathering
  ○ Identify application’s stakeholders
    • What a stakeholder is?
    • The roles of stakeholders in context of security assessment
  ○ Acquire documentation, business and security requirements
    • Schemas, diagrams, manuals, etc.. (public)
  ○ Application use cases, if available
  ○ Define the target environment
    • Production VS. test targets
  ○ Search Engine Hacking
    • LAB - Google Hacking laboratory sessions
• Step 3 - Application Enumeration
  ○ Exploring the application’s attack surface, an introduction
  ○ Hosted Application Enumeration
    • Introduction to Virtual Hosting
    • LAB - Using Bing Search to identify multiple virtual hosts
  ○ Server and Technologies Fingerprinting
    • Direct interaction with web/application server
    • Web/application server fingerprinting
    • LAB - Fingerprinting web server with httprint
    • LAB - Identify default resources using DirBuster and FuzzDB lists
3rd Party Application and plugins Identification (e.g. WordPress, Joomla)
  ● LAB - using BlindElephant to fingerprint a web application

Application Spidering
  ● Definition of spidering/crawling
    ○ Differences between static and dynamic resources
    ○ Review web pages comments and Metadata
  ● LAB - spidering a web app with Burp Suite Spider
  ● LAB - Web fuzzing with Burp Suite Intruder

  ○ Application Flow Charting
    ■ Application dynamic resources VS application states
    ■ Application states analysis
      ● Perform a match analysis on provided documentations
      ● Testing multi-step processes
      ● LAB - Amazon flowcharting with a sequence diagram

DAY 03

● Recap of the previous day
● Module introduction
  ○ Overview of the first day
● Step 4, part I - Testing: Web Application Scanning
  ○ Internals of web application scanners
  ○ Web Application scanners
    ■ Commercial scanners
    ■ Open source solution
  ○ Tuning and running a web application scanning
    ■ Pre-scan analysis
      ● Collecting the target URLs
    ■ Tool setup
    ■ Common issues and pitfalls
      ● Loops, sessions and multi-step scanning
  ○ LAB - Scanning a web application with nikto web scanner
  ○ LAB - Scanning a web application with SkipFish
  ○ LAB - Scanning a web application with Burp Suite Scanner Professional
  ○ LAB - Scanning a web application with Tenable Nessus Scanner
DAY 04

- Recap of the previous day
- Module introduction
  - Overview of the first day
- Step 4, Part II - Vulnerabilities Analysis
  - Scanner output analysis
  - Identify false positive
  - Testing the identified vulnerabilities
  - LAB - Identify false positives and develop simple PoCs
- Step 5 - Reporting
  - Vulnerabilities Reporting
  - Vulnerability Impact Evaluation
    - (re)Introducing the concept of security risk
    - Introducing the OWASP Risk Rating Methodology
    - LAB - risk evaluation of vulns identified by the scanner
- Secure Software Development
  - Introduction to SDLC
  - The role of Application Vulnerability Assessments in SDLC
- Mobile Devices Vulnerabilities
  - Introduction to Mobile Devices Vulnerabilities
- References & Tools