Security Testing Online Course

Course Summary:

- ⇒ In detailed, easy, step by step, real time, practical and well organized Course
- ⇒ The trainer is a Passionate Cyber Security Professional having 10 Plus years of experience in information security testing.
- ⇒ He is one of those few Security professional who holds internationally renowned CISSP and CISA Certifications besides CEH.
- ⇒ No pre-requisites required for this Training.
- ⇒ This course is appropriate for software development and testing professionals who want to begin doing security testing as part of their assurance activities.
- ⇒ Practical Hands-on training will be provided using various Security Testing Tools by a real-time expert.
- ⇒ This is a beginner to advanced course on Security Testing (Penetration Testing)
- ⇒ Assignment/Tasks will be provided to build your confidence.
- ⇒ Most of the tools will be covered in this course – Check the contents section in this page for more details (Course Differentiator)
- ⇒ Real time Project with practical demonstration of identifying various vulnerabilities (Course Differentiator)
- ⇒ Training videos and PPT slides will be shared at the end of every session

Course Contents:

⇒ **Introduction**

- What is Security Testing?
- Vulnerability, Threat, and Risk
- Importance/Purpose of Security Testing
  - Importance of Security Testing
  - Major Security Breaches

⇒ **Basic Security Testing Concepts & Web Application Penetration Testing (Hands-on)**

- **CIA Triad**
  - Confidentiality
  - Integrity
  - Availability
- **HTTP/HTTPS Protocols**
  - Basic Features
    - Protocol Methods
      - GET
      - POST
      - PUT
      - HEAD
      - DELETE
      - CONNECT
      - OPTIONS
      - TRACE
    - Protocol Response Codes
      - 1XX Informational Responses
      - 2XX Success Responses
      - 3XX Redirection Responses
      - 4XX Client Errors
      - 5XX Server Errors
    - Protocol Headers
    - Client-Server Architecture
    - HTTP versus HTTPS
- **Cryptography**
  - Encoding
    - ASCII
    - UNICODE
    - URL ENCODING
    - base64
  - Decoding
  - Encryption

- Decryption
- Symmetric Encryption
  - AES
  - DES
  - 3DES
- Asymmetric Encryption
  - RSA
  - DSA
- Hashing
  - MD5
  - SHA1
  - SHA2
- Encryption versus Encoding versus Hashing

- **Same Origin Policy**
- **Cookies**
  - Session Cookies
  - Persistent Cookies
- **Sessions**
  - Cookies versus Sessions
- **Validations**
  - Input Validations
  - Output Encoding
  - Black List Validation
  - White List Validation
  - Black List versus White List Validation
  - Client Side Validation
  - Server-Side Validation
- **Secure SDLC Process**
  - SDLC Process versus Secure SDLC Process
  - Advantages of Secured SDLC Process
- **Threat Modelling**
  - STRIDE Methodology
    - SPOOFING
    - TAMPERING

- REPUDIATION
- INFORMATION DISCLOSURE
- ELEVATION OF PRIVILEGES

- **Security Testing Process and Methodology**
- **Secured Socket Layer**
  - SSL
  - TLS
  - SSL Versus TLS
  - SSL/TLS Versions
  - SSL Handshake Process
- **Authentication & Authorization**
  - Authentication
  - Authorization
  - Authentication versus Authorization
- **Phases of Security Testing**
  - Information Gathering
  - Planning and Analysis
  - Vulnerability Detection
  - Penetration Tests and Attacks
  - Reporting
- **OWASP Top Vulnerabilities**
  - What is Vulnerability?
  - What is Threat?
  - What is Risk?
  - Types of Vulnerabilities
  - Vulnerability Scanning
- **SQL Injection**
  - What is SQL?
  - SQL Query Generation
  - What is SQL Injection?
  - SQL Injection Types
    - Error Based
    - Non Error Based
    - Time Based

- SQL Injection Impact / Consequences
- SQL Injection Payloads
- Where to Test SQL Injections?

- **Vulnerable Application and SQL Injection Demonstration**
  - Examples for SQL Injections
  - Countermeasures
  - Recommendations Remedy/Fix
  - XAAMP Installation and Configuration
  - BWAAP Demo Download and Configuration
- **SQL Injection Tools**
  - SQLMap tool:
    - SQLMap Installation
    - Demonstrating the identification of SQL Injections using SQLMap tool
  - BurpSuite Tool
    - BurpSuite Installation
    - Demonstrating the identification of SQL Injections using BurpSuite tool
- Other SQL Injection Stuff:
  - SQL Injection and Code Examples
  - Exercises / Assignments
- **Cross Site Scripting (XSS)**
  - What is Cross Site Scripting?
  - Consequences of Cross Site Scripting
  - Where to Test Cross Site Scripting?
  - Cross Site Scripting Payloads
  - Countermeasures
  - Recommendations
  - Remedy / Fix
  - Cross Site Scripting Types
    - Reflected XSS
    - Stored XSS
    - DOM Based XSS
  - XSS and BurpSuite Tool
  - Demonstration using Tools
  - XSS Examples / Exercises / Assignments

- **Cross Site Request Forgery (CSRF)**
  - What is Cross Site Request Forgery?
  - Consequences
  - Preconditions
  - Where to Test Payloads?
  - Countermeasures
  - Recommendations
  - Remedy / Fix
  - CSRF and BurpSuite Tool
  - Demonstration using Tools
  - CSRF Examples Exercises / Assignments
- **Insecure Direct Object Reference**
  - What is Insecure Direct Object Reference?
  - Consequences
  - Where to Test?
  - Payloads
  - Countermeasures
  - Recommendations
  - Remedy / Fix
  - Demonstration using Tools
  - Examples / Exercises / Assignments
- **Failure to Restrict URLs**
  - What is it?
  - Consequence
  - Where to Test?
  - Payloads
  - Countermeasures
  - Recommendations
  - Remedy / Fix
  - Demonstration using Tools
  - Examples / Exercises / Assignments

- **Security Misconfiguration**
  - What is it?
  - Consequences
  - Where to Test?
  - Payloads
  - Countermeasures
  - Recommendations
  - Remedy / Fix
  - Demonstration using Tools
  - Examples / Exercises / Assignments
- **Unvalidated redirects and forwards**
  - What is it?
  - Consequences
  - Where to Test?
  - Payloads
  - Countermeasures
  - Recommendations
  - Remedy / Fix
  - Demonstration using Tools
  - Examples / Exercises / Assignments
- **Broken Authentication and Session Management**
  - What is it?
  - Consequences
  - Where to Test ?
  - Payloads
  - Countermeasures
  - Recommendations
  - Remedy / Fix
  - Demonstration using Tools
  - Examples / Exercises / Assignments

- **Using components and known vulnerabilities**
  - What is it?
  - Consequences
  - Where to Test?
  - Payloads
  - Countermeasures
  - Recommendations
  - Remedy / Fix
  - Demonstration using Tools
  - Examples / Exercises / Assignments
- **Sensitive Data Exposure**
  - What is it?
  - Consequences
  - Where to Test?
  - Payloads
  - Countermeasures
  - Recommendations
  - Remedy / Fix
  - Demonstration using Tools
  - Examples / Exercises / Assignments
- **Insecure Logging and Storage**
  - What is it?
  - Consequences
  - Where to Test?
  - Payloads
  - Countermeasures
  - Recommendations
  - Remedy / Fix
  - Demonstration using Tools
  - Examples / Exercises / Assignments
- **Insecure Communication**
  - What is it?
  - Consequences
  - Where to Test?

    - Payloads
    - Countermeasures
    - Recommendations
    - Remedy / Fix
    - Demonstration using Tools
    - Examples / Exercises / Assignments
- **Vulnerable SSL/TLS Versions**
    - What is it?
    - Consequences
    - Where to Test?
    - Payloads
    - Countermeasures
    - Recommendations
    - Remedy / Fix
    - Demonstration using Tools
    - Examples / Exercises / Assignments
- XML External Entity
    - What is it?
    - Consequences
    - Where to Test?
    - Payloads
    - Countermeasures
    - Recommendations
    - Remedy / Fix
    - Demonstration using Tools
    - Examples / Exercises / Assignments
- **Authentication related tests**
    - Credentials transport over an encrypted channel/Insecure Communication
    - Testing for user enumeration
    - Default or guessable (dictionary) user account
    - Testing for Brute Force
    - Testing for Bypassing authentication schema
    - Testing for Vulnerable remember password and password reset
    - Testing for Logout and Browser Cache Management

- Testing for CAPTCHA
- Insufficient Password Policy
- Insufficient Password change Policy
- Password Stored in Plane test and Password History

- **Authorization related tests**
  - Path Traversals
  - Bypassing Authorization schema
  - Privilege Escalation
- **Session Management Testing**
  - Session Hijacking, Session Fixation, Session Timeout, Session replay and Session Invalidation
  - Exposed Session Variables
- **Configuration related tests**
  - Missing Http Only and Secure Flags
  - Clickjacking
  - HTTP Strict transport Security Header
  - Unsafe CORS Policy- HTML5
  - Cookie Scoped to parent domain
  - Improper error message
- **Malicious File Upload**
  - Introduction to various Vulnerability Scanners
  - Scanning application using BurpSuite and False positive elimination
  - Bypassing client-Side Validations
  - Risk Rating and Report preparation
- **Mobile Security Testing (Hands-on)**
  - Jail breaking/Rooting
  - Creating Virtual Devices
  - Installing the APK/IPA file
  - Decompiling the file
  - SSH the device
  - Local data storage for information leakage
  - Intercepting the request using BurpSuite
  - Reverse Engineering
  - Demonstration using Tools
  - Examples / Exercises / Assignments

- **Network Security Testing (Hands-on)**
  - Basic Networking Concepts
    - OSI Layers
    - TCP VS UDP
    - What is an IP
    - IP Address Classes
    - IP V4 VS IP V6
    - Different Ports and Protocols
    - Hubs, Switches, Routers, Firewalls and DMZ
  - Network Security Testing Methodology
  - Scanning a network using Nessus
  - Scanning and evidence gathering using Nmap
  - Internal Vs External Network Security Testing
  - Report Preparation
- **Tools Covered in this course:**
  - BurpSuite
  - ZAP
  - Acunetix
  - Appscan
  - Sslyze
  - Sqlmap
  - Nmap
  - Nessus
  - SSLscan
  - GenyMotion
  - ADT Bundle
  - Android studio
  - Drozer
  - Androbugs
  - Some password cracking tools
  - Kali Linux and Metasploit framework [Practical demonstration of various Exploits]
- **Real Time Project**
- **Interview Questions with Answers**

End of the Course Contents