MASTERCLASS: PEN TESTING AND SECURING MOBILE AND WEB APPLICATIONS

DURATION: 3 DAYS

COURSE OVERVIEW

The course teaches mobile and web application security concepts, including the techniques on how to attack and how to respond with an appropriate countermeasure implementation. Our course has been developed around professional penetration testing and security awareness in the business and IT fields. To make sure that all participants gain the necessary security knowledge, our classes have an intensive hands-on format. Every topic is supported with virtual labs instructions and code examples. Knowledge and concepts of penetration testing are universal in all programing languages nevertheless exercises and code examples require Microsoft .Net programing skills and android development basics.

TARGET AUDIENCE

Developers, web developers, mobile solution developers, solution architects, security professionals with strong programing skills and other people responsible for implementing security of development process or application security.

COURSE OBJECTIVES

1. Recognize the security risks that can be found in modern applications
2. Perform pen tests on web application and web API's
3. Understand Security concepts in relation to Mobile Android Applications
4. Test the end to end mobile and web application solution

COURSE CONTENT

Module 1: OWASP Top 10 Application Security Risks

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XXE
5. Broken Access Control
6. Security Misconfiguration

7. Cross-Site Scripting
8. Insecure Deserialization
9. Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

Module 2: Analysis of Web Application Security

In this module, you will learn how to perform series of web applications and web API penetration tests. Additionally, you will learn the most effective ways of securing them.

1. Methodologies of Web Application testing
2. Black Box Analysis
3. White Box Analysis
4. Automating penetration tests with OWASP ZAP
5. Web Application Firewall: Traditional vs Anomaly detection modes

Module 3: Analysis of Android Application Security

This module focuses on mobile Android applications, its general design, security concepts and different approaches to penetration tests and security, especially independent from OS version.

1. System architecture
2. Android OS security features
3. Black and White box tests for mobile
4. Android storage solutions
5. Encryption in App and OS

Module 4: End to End solution testing

This module covers different methods of penetration testing of whole solutions regardless of technology used as development platform.

1. Methodologies, solutions and tools
2. Fuzzy testing for Mobile applications
3. Fuzzy testing for Web API
4. Performance testing

Module 5: Use cases and discussion

This module covers discussion about security solutions specific in different technologies. It also demonstrates practical and complete use case of penetration testing and solution in 'hands-on labs' environment.

COURSE PREREQUISITES

Microsoft .Net programing skills and android development basics

TEST CERTIFICATION

Recommended as preparation for the following exams:

There is no specific exam aligned to this course, however all attendees will receive an online Certificate of Attendance