Web Application Security Fundamentals

Information

Length:	1.0 Day
__Ref:	TK330G-X
Delivery method:	ClassroomInstructor Led Online
Price:	EUR

Overview

This course focuses on common web security attack vectors, how attackers exploit them, and how to prevent the exploits. It also introduces the Open Web Application Security Project (OWASP) as an industry standard security resource. Students learn through hands-on labs how to exploit web security vulnerabilities.

Public

This basic course is for web developers, quality assurance specialists, security auditors, and users who are new to IBM Security AppScan products.

Prerequisits

Before taking this course, make sure that you have the following skills:

- Basic knowledge of internet technologies such as HTTP**and** TCP/IP
- Basic knowledge of web application technologies such as SQL**and** operating systems

Objective

- Discuss common web application security issues and the organizations and testing techniques that can help prevent them
- Describe basic web application components
- Discuss the OWASP web application security attack classifications:
  - Injection
  - Broken authentication and session management
  - Cross-site scripting
  - Insecure direct object references
  - Security misconfiguration
  - Sensitive data exposure
  - Missing function level access control

    - Cross-site request forgery
    - Using components with known vulnerabilities
    - Unvalidated redirects and forwards

- Use vulnerability testing and threat modeling to implement web application security throughout the software development life cycle

Topics

- Unit 1: Introduction to web application security problems
- Unit 2: Web application security basics
- Unit 3: Injection flaws
- Unit 4: Broken authentication and session management
- Unit 5: Cross-site scripting
- Unit 6: Insecure direct object references
- Unit 7: Security misconfiguration
- Unit 8: Sensitive data exposure
- Unit 9: Missing function-level access control
- Unit 10: Cross-site request forgery
- Unit 11: Using components with known vulnerabilities
- Unit 12: Unvalidated redirects and forwards
- Unit 13: Integrating security into the software development lifecycle