Updated 07/26/2023

Sign up

Web Application Security Training

3 days (21 hours)

PRESENTATION

This Web Application Security course focuses on the most common Web vulnerabilities, so you can detect attacks and secure your Web applications.
Thanks to our training, your team will learn how to identify the most common vulnerabilities in web applications, and understand how different attacks work, so as to prevent risks to your business. They will also learn how to implement simple security measures and test the security of your applications. You'll also be able to configure a Web server to encrypt Web traffic using HTTPS. This training will enable your company to bring a level of security to deployed applications such as extranet services and messaging. After this course, you'll have the keys to protecting an online service, with examples of appropriate countermeasures and attacks. Depending on progress, the following topics in particular may be covered: brute force and fuzzing attacks, partitioning and access control, exploitation of blind SQL injections, Cross-Site Scripting (XSS).

OBJECTIVES

- Understanding security vulnerabilities
- Understanding attack sequences
- Testing the security of your web applications

TARGET AUDIENCE

- Developers
- Project managers
- Network/system administrators
- Sliders
- Ethical hackers

Prerequisites

- Basic knowledge of web security
- Knowledge of a programming language

OUR WEB APPLICATION SECURITY TRAINING PROGRAM

INTRODUCTION

- The web security ecosystem
- The different standards
- The various laws
- Reference systems
- Threat overview
- Vulnerabilities
    - Major risks
    - Injection attack
    - Attack on sessions
    - Attack on standard configurations
- Client-side attacks
    - Cross Site Scripting (XSS)
    - Session management and authentication
    - Phishing

THE DIFFERENT COMPONENTS OF A WEB APP

- What is the HTTP front-end server?
    - Its role
    - His weaknesses
- HTTP protocol
    - Queries
    - The answers
    - HTTP codes
    - HTTPS
- Intrinsic risks
- Market players
- The Customer
- The Server
- URLs
    - The anatomy of a URL
    - Open redirect vulnerabilities
- Headers
- The different methods
- Status code

SECURE DEVELOPMENT

- What is secure development?
- Roles
    - Customer side
    - Safety
    - Ergonomics
- Buffer Overflow" attack
- The various development rules to be observed
- Residual risks
    - Headers
    - Malformed URL
    - Cookie Poisoning

APPLICATION HARDENING

- Secure authentication
- Password management
    - Status code modification
    - Dynamic salting
- Encoding
    - Inputs
    - Outings
- Management
    - Logs
    - Sessions

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.