+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 24/08/2023

Sign up

OWASP Java Training

3 days (21 hours)

PRESENTATION

This OWASP Java training course is an advanced course in Java development security, enabling you to optimize the security of your web applications, and in particular your cloud products. Based on the best standards and practices on the market. This course teaches you the best practices to adopt to ensure the security of your developments. Following this course, your development teams will have a broad and exhaustive knowledge of the fundamentals of good web security, thanks to a better understanding of the Java Secure Coding Rules with CERT Oracle Java Secure Coding, a better understanding of how HTTP works, and the correct use of security technologies such as encryption or digital certificates. The program also provides detailed instruction on how to secure servers, applications, web services and Ajax architecture. The course alternates theory and case studies to ensure effective operational implementation. At the end of the course, an assessment will be carried out to measure the assimilation of the concepts covered. As always, we will be using the latest technologies: Java SE 18. We can also offer you OWASP training with PHP.

OBJECTIVES

- Master and understand the most common web vulnerabilities
- Java security mechanisms
- Design, develop and test web applications that provide reliable web services
- Improving the security of the Ajax protocol
- Identify security weaknesses and threats in your applications

TARGET AUDIENCE

Developers, Technical architects, Project managers

Prerequisites

- Good knowledge of Windows and Linux/UNIX

- Good TCP/IP skills
- Good command of HTTP, Javascript and development

Further information

We offer OWASP security training with ASP.NET We also offer Java training and Java training on new features

PROGRAM FOR OUR OWASP SECURITY TRAINING WITH JAVA

BEFORE YOU START

- Web security fundamentals
- Secure Coding .NET & C# rules
- Java Secure Coding rules with CERT Oracle Java Secure

WEB SECURITY FUNDAMENTALS

- Application security requirements
- Overview of how HTTP works
- Security technologies

IMPROVE WEB SERVER PROTECTION

- Configuration management
- Server authentication
- File system permissions
- Encrypting Web traffic

SECURING WEB APPLICATIONS

- Web application security
- Input validation
- Injection faults
- Cross site scripting (XSS)
- Authentication and session management
- Insecure storage and communication
- URL access restriction
- Unsecured direct object reference

- Cross-site request forgery
- Information leakage and error handling

IMPROVE AJAX SECURITY

- Ajax principles
- Identifying increased risk exposure

PROTECT YOUR WEB SERVICES

- How Web services work
- XML vulnerabilities in Web services
- Message security

IDENTIFY APPLICATION WEAKNESSES

- Manual test tools
- Web application analysis tools

BEST PRACTICES FOR SECURE JAVA APPLICATION DEVELOPMENT

- Securing the JVM
- Performance protection
- Control
- Obfuscation
- JAAS
- CERT Oracle Secure Coding Rules

Companies concerned

This training 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.