Publication date : 07/11/2024

Course : Java, .NET and PHP application security

Practical course - 3d - 21h00 - Ref. ANP
Price : 2460 CHF E.T.

This highly practical training course will enable you to grasp the security management mechanisms offered by Java, .NET and PHP. You'll see how to implement security at the Java virtual machine level and master the security mechanisms of the .NET and PHP platforms.

Teaching objectives

At the end of the training, the participant will be able to:

- Integrating safety into development right from the design stage
- Identify potential development flaws
- Developing more secure applications
- Implementing security at the Java virtual machine level
- Master the security mechanisms of the .NET and PHP platforms

Intended audience

Developers, application architects, project managers who need to secure applications.

Prerequisites

Have completed the "Develop secure applications" training course.

Course schedule

1 Java virtual machine security

- Loading classes. Concept of "sandbox".
- SecurityManager, AccessController and permissions definition (.policy files).
- Create permissions with Java Security Permission.
- Mechanisms to protect bytecode integrity, decompilation and code obfuscation.
- Applet security features.

Hands-on work

Definition of specific .policies.

PARTICIPANTS

Developers, application architects, project managers who need to secure applications.

PREREQUISITES

Have completed the "Develop secure applications" training course.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

2 Java Authentication and Authorization Service

- JAAS architecture.
- Authentication via PAM, notion of Subject and Principal.
- Permissions management, .policy files.
- Using JAAS with Unix or Windows, JNDI, Kerberos and Keystore. SSO support.

Hands-on work

Configure access control policy, implement authentication.

3 Security issues in .NET

- Definition of safety.
- Authentication, Protection, Encryption.
- .NET security tools.
- Runtime security, authentication, data and access protection.
- Types of threats, validation of data entered.

4 .NET Framework security

- Protection of assembly contents.
- Protection of program execution.
- Deployment of a CLR security strategy.
- Security strategy and application deployment. Principle of using "proofs".
- Execution rules according to application origin.
- What's new in .NET4.
- Total/partial trust.

Hands-on work

Retrieve proofs presented by an assembly. Sign/modify an assembly.

5 .NET code security

- Transparent security code, security critic and secure critic.
- What are the code's access authorizations?
- How to obfuscate code. Encrypting configuration information.
- Implement declarative/imperative management of security mechanisms.
- Restrict/verify program execution rights.
- How to implement role-based security management.

Hands-on work

Code access authorization.

6 The right settings for securing PHP

- The PHP.ini configuration file. Identify sensitive directives, sessions and errors.
- How to set up script protection. Physical protection. Remote or on-the-fly script execution.
- Cookies and sessions.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

7 Database security

- What are the potential database vulnerabilities? Administration. Storage.
- SQL injection" attacks. Principle and countermeasures. Stored procedures and parameterized queries. Limitations.
- What are the access files? Organization and default values. Anonymous access and protocols.

8 Securing the use of PHP extensions

- Email. Spam via a contact form: injections and countermeasures.
- How to implement network access using PHP. Sequential and recursive calls. Stealth attacks.

9 Web application vulnerabilities

- Why are Web applications more exposed? The major risks of Web applications according to OWASP.
- Cross Site Scripting" or XSS attacks. Why are they on the rise? How can they be avoided?
- Injection attacks (command injection, SQL injection, LDAP injection, etc.). Attacks on sessions.
- Exploitation of HTTP front-end vulnerabilities (Nimda worm, Unicode flaw). Attacks on standard configurations
- How to search for vulnerabilities.
- Search for the most widespread vulnerabilities. Cross-Site Scripting. SQL injection.
- Application logic errors. Buffer overflow. Execution of arbitrary commands.

10 Best practices

- What are the different types of input? How do I validate entries?
- What kind of operations can be performed on digital types?
- Classes and exceptions.
- Multi-threading and synchronization.
- I/O, serialization.
- Know how to manage permissions.

Hands-on work

The practical exercises have been designed to illustrate all the elements of the language and to systematically implement the concepts in order to master the security mechanisms.