Publication date : 02/12/2024

Course : PHP, securing your applications

For versions 8, 7 and 5

Practical course - 3d - 21h00 - Ref. PSE

Price : 2150 CHF E.T.

5 / 5

By its very nature, a dynamic Web page service opens many doors to the outside world. For developers, it's vital to be aware of the types of attack to which their code is potentially exposed, and to know how to deal with them - the dual objective of this course.

Teaching objectives

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

- Be aware of the types of attack to which your code may be exposed
- Integrating safety into development right from the design stage
- Identify potential development flaws
- Developing more secure applications

Intended audience

Developers looking to build more secure PHP applications.

Prerequisites

Good knowledge of PHP and SQL. Basic knowledge of JavaScript.

Practical details

Hands-on work

Windows workstations equipped with Apache2 servers with PHP, MySql, Oracle, LDAP, FTP and mail will be made available to participants.

Teaching methods

Active pedagogy based on examples, demonstrations, experience sharing, case studies and assessment of learning throughout the course.

Course schedule

PARTICIPANTS

Developers looking to build more secure PHP applications.

PREREQUISITES

Good knowledge of PHP and SQL. Basic knowledge of JavaScript.

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.

1 Introduction

- Presentation of risks.
- Data destruction.
- Site hijacking.
- Publication of confidential data.
- Abuse of resources.
- Identity theft.
- Safety Plan: Design, Development and Maintenance.

2 Web pages

- XSS principles and protection methods. Search engine.
- CSRF: principle and countermeasures. Database viruses.

3 Forms: the big door

- Vulnerabilities. Validation and limitations of the JavaScript approach. Chaining, HTTP and Ajax attacks. Countermeasures.
- Input validation. Tests and list principles. Regular expressions, standards and filters.
- Upload. Vulnerabilities and countermeasures.

4 Cookies and sessions

- Cookies. Principles and risks. JavaScript handling. Cookie tables.
- Sessions. Cookie vs. Header mode. Session theft principle.

5 Securing PHP: the right settings

- PHP.ini. Sensitive directives, sessions and errors.
- Protect scripts. Physical protection. Remote or on-the-fly script execution.

6 Databases

- Potential vulnerabilities. Administration. Storage.
- SQL injections. Principle and countermeasures. Stored procedures and parameterized queries. Limitations.
- Access files. Organization and default values. Anonymous access and protocols.

7 Securing the use of extensions

- Email. Spam via a contact form: injections and countermeasures.
- PHP network access. Sequential and recursive calls. Stealth attack.

8 General considerations

- BFA. Principle. Identification and countermeasures.
- Phishing. Principle and user training.
- DoS. Quotas and load management.
- Passwords. Reinforcement and storage .
- Encryption and signature. Encryption/decryption: PHP and MySQL implementation.
- Tricks. Honeypot, Obfuscation and Reverse Turing.
- Frameworks and software bricks. Security management in composite developments.
- Security audits. Basic methodology, cross-testing and audit reporting.

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.

Dates and locations

REMOTE CLASS
2026 : 25 Mar., 8 June, 21 Oct.