Publication date : 02/29/2024

Course : Web application security, advanced

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

4,6 / 5

This advanced course will enable you to enhance your skills in protecting yourself and reacting more effectively to the many threats posed by the Web. You'll learn how to audit the security of your applications, test them and implement the most appropriate countermeasures.

Teaching objectives

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

- Learn how to set up an audit of a Web application
- Set up a Web server with vulnerabilities to observe its behavior
- Implement security measures for Web applications
- Implementing a private certification authority with certificate integration in an application
- Use a web spider to detect broken links and pages with or without authentication

Intended audience

Network and systems administrators, webmasters.

Prerequisites

Good knowledge of systems and networks, basic knowledge of development or knowledge equivalent to that provided by the course "Web application security" ref. SER.

Practical details

Exercise

Numerous exercises and case studies will be proposed throughout the course.

Teaching methods

Theoretical foundations illustrated by practical exercises.

Course schedule

PARTICIPANTS

Network and systems administrators, webmasters.

PREREQUISITES

Good knowledge of systems and networks, basic knowledge of development or knowledge equivalent to that provided by the course "Web application security" ref. SER.

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 Reminder of the main security vulnerabilities

- Cross-Site Scripting (XSS) attack.
- Command injection and SQL injection.
- Denial of Service (DoS) attacks.
- Distributed Denial of Service (DDoS).
- Buffer overflow.
- The Open Web Application Security Project (OWASP).

Hands-on work

Set up a Web server with vulnerabilities to observe its behavior.
Demonstrate how to exploit a buffer overflow.

2 Application security

- Basic concept and importance.
- The accounts created to run the tests.
- Can we do without fictitious files?
- Are test and development sequences still present in production?

3 Auditing and securing a Web application

- Audit approach and implementation. Managing database interaction.
- Implementing secure authentication. Exploiting an authentication flaw.
- Error, exception and log management.
- Analyze and correlate log information.
- Best practices for secure forms. Example of a poorly developed form.

Hands-on work

Implementation of a three-tier infrastructure: client, Web server and databases. Simulation of an attack attempt. Analysis and solution.

4 Encryption

- A reminder of the basic principles.
- Implement encryption in an application. Possible uses.
- Test whether an application is properly protected by encryption.
- Encryption applications on the market.

Hands-on work

Implementation of a private certification authority with certificate integration in an application.

5 Testing applications

- How to test before going live.
- Fingerprinting: identification of server characteristics (web engine, framework, applications).
- Use a web spider to detect broken links and pages with or without authentication and encryption.
- How to measure application availability with a simulation.

Hands-on work

Example of attempted attacks and fingerprinting. How to write a web spider to detect broken links. Checking page authentication.

Dates and locations

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.

REMOTE CLASS
2026 : 25 Mar., 27 May, 5 Oct., 7 Dec.