Publication date : 07/24/2024

Course : Web application security, overview

Seminar - 2d - 14h00 - Ref. SEW
Price : 1850 € E.T.

This seminar provides an overview of Web threats. It details vulnerabilities in browsers, social networks, SSL/TLS and X509 certificates, as well as Java EE, .NET and PHP applications. It presents solutions for protecting and controlling application security.

Teaching objectives

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

- Identify security threats to Web applications
- Web security protocols
- Understanding attack typologies
- Securing Web applications

Intended audience

CIOs, CISOs, security managers, developers, designers, project managers integrating security constraints, network, IT and system managers or administrators.

Prerequisites

Basic computer and network skills.

Course schedule

1 Web application threats and vulnerabilities

- Major Web application risks according to IBM X-Force and OWASP.
- Cross Site Scripting (XSS), injection and session-based attacks.
- Fault propagation with a Web Worm.
- Attacks on standard configurations.

PARTICIPANTS

CIOs, CISOs, security managers, developers, designers, project managers integrating security constraints, network, IT and system managers or administrators.

PREREQUISITES

Basic computer and network skills.

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 SSL and TLS security protocols

- SSL v2/v3 and TLS, PKI, X509 certificates, certification authority.
- SSL's impact on UTM and IDS/IPS firewall security.
- SSL/TLS vulnerabilities and attacks. Techniques for capturing and analyzing SSL flows.
- HTTPS stripping attack on secure links.
- Attacks on X509 certificates, OCSP protocol.
- SSL and Web application performance.

3 User- and browser-targeted attacks

- Attacks on Web browsers, Rootkit.
- Smartphone security for surfing the Net.
- Malicious code and social networks.
- Social Engineering techniques.

4 Targeted attacks on authentication

- Authentication via HTTP, SSL with client X509 certificate.
- Implement strong software-based authentication.
- Non-intrusive (agentless) Web SSO solution.
- Main attacks on authentication.

5 Web services security

- Protocols, security standards XML Encryption, XML Signature, WS-Security/Reliability.
- Injection (XML injection...), brute force or replay attacks.
- Application firewalls for Web Services.
- Main players and products on the market.

6 Efficiently securing Web applications

- Hardening: securing the system and HTTP server.
- Virtualization and security for Web applications.
- .NET, PHP and Java environments. The 5 SDL phases.
- Fuzzing techniques. Qualify your application with ASVS.
- WAF: what efficiency, what performance?

7 Controlling Web application security

- Pentest, security audit, vulnerability scanners.
- Organize an effective technology watch.
- Reporting security incidents.

Demonstration

Implementation of a Web server with X509 EV certificate: analysis of protocol exchanges. Exploitation of a critical security flaw on the HTTP front-end. HTTPS Stripping attack.

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 : 28 May, 8 Sep., 26 Nov.

PARIS LA DÉFENSE
2026 : 28 May, 8 Sep., 26 Nov.