Securing Web Applications, Services, and Servers Training

Course: **00106**

Filter: **Beginner**

Duration: **20 hours**

Category:: **Software Application Security**

Price: **3000,00 €**

About Course

This Full Stack Cybersecurity Training for Web Apps and Services course provides in-depth, hands-on experience securing Web-based applications and their servers. You will gain in-depth experience securing web services and learn how to integrate robust security measures into the web application development process by adopting proven architectures and best practices. This web service security course includes the OWASP top 10 most critical web application security risks and how to remediate them.

What you'll learn

- Implement and test secure web applications in your organization
- Identify, diagnose, and remediate the OWASP top ten web application security risks
- Configure a web server to encrypt web traffic with HTTPS
- Protect Ajax-powered applications and prevent JSON data theft
- Secure XML web services with WS-Security

Pre-requisites

- Basic knowledge of Web application operation and Web server administration is assumed. For example, you should understand Web browser/server operation, session management and basic HTML. In addition, experience with server-side Web application development and security knowledge is helpful.

Curriculum

Module 1: Setting the Stage

- Defining threats to your web assets
- Surveying the legal landscape and privacy issues

Module 2: Establishing Security Fundamentals

- Modeling web security
- Encrypting and hashing

Module 3: Augmenting Web Server Security

- Configuring security for HTTP services
- Securing communication with SSL/TLS
- Detecting unauthorized modification of content

Module 4: Implementing Web Application Security

- Employing OWASP resources
- Securing database and application interaction
- Managing session authentication
- Controlling information leakage
- Performing input validation

Module 5: Enhancing Ajax Security

- Ajax features
- Assessing risks and evaluating threats
- Diagnosing XML vulnerabilities
- Protecting the SOAP message exchange

Module 6: Scanning Applications for Weaknesses

- Operating and configuring scanners

- Detecting application flaws

Module 7: Best Practices for Web Security

- Adopting standards
- Managing network security