Web Application Security

Hands-on course of 3 days - 21h
Ref.: SER - Price 2024: CHF2 390 (excl. taxes)

EDUCATIONAL OBJECTIVES

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

Identify the most common vulnerabilities in web applications

Understand how an attack proceeds

Implement simple security measures for web applications

Configure a web server to encrypt web traffic with HTTPS

Test the security of your web applications

HANDS-ON WORK

Secure, protected online sites (multi-DMZ firewall) will be deployed, SSL acceleration, a HTTP protocol analysis proxy, an HTTP(S) flow injector, strong certificate-based authentication, attack tools on HTTPS flows.

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.

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.

THE PROGRAMME

last updated: 07/2021

1) Introduction

- Statistics and changes in web-related vulnerabilities according to IBM X-Force and OWASP.
- Changes in protocol and application attacks.
- The world of hackers: Who are they? What are their motives, their means?

2) Components of a Web application.

- Elements of an N-tier application.
- The HTTP front-end server, its role, and its weaknesses.
- The intrinsic risks of these components.
- Major players on the market.

3) The HTTP protocol in detail.

- Refreshers on TCP, HTTP, persistence, and pipelining.
- The PDUs GET, POST, PUT, DELETE, HEAD, and TRACE.
- Header fields, status codes 1xx to 5xx.
- Redirection, virtual host, proxy cache, and tunneling.
- Cookies, attributes, corresponding options.
- Authentications (Basic, Improved Digest, etc.).
- HTTP acceleration, proxy, web balancing.
- HTTP Request Smuggling and HTTP Response Splitting protocol attacks.

Hands-on work : Installation and use of the Wireshark network analyzer. Using a special HTTP analysis proxy.

4) Vulnerabilities of Web applications

- Why are Web applications more vulnerable?
- Major risks of Web applications according to OWASP (Top Ten 2017).
- "Cross Site Scripting" or XSS attacks Why are they growing? How can they be avoided?
- Injection attacks (injection commands, SQL Injection, LDAP injection, etc.).
- Session attacks (cookie poisoning, session hijacking, etc.).
- Exploiting vulnerabilities on the HTTP front-end (Nimda worm, Unicode exploit, etc.).

- Attacks on standard configurations (Default Password, Directory Traversal, etc.).
Hands-on work : Cross Site Scripting attack. Exploiting a vulnerability in the http front-end. Bypassing authentication with an SQL query injection.

5) The network firewall in protecting HTTP applications

- The network firewall, its role, and its functions.
- How many DMZs for an N-Tier architecture?
- Why isn't the network firewall suitable for protecting a Web application?

6) Making flows secure with SSL/TLS

- Reminders of cryptographic techniques used in SSL and TLS.
- Managing your server certificates, the X509 standard.
- What is the new X509 EV certificate good for?
- What certification authority should you choose?
- SSL flow capture and analysis techniques.
- The main vulnerabilities of X509 certificates.
- Using a reverse proxy for SSL acceleration.
- The benefit of HSM crypto-hardware cards.
Hands-on work : Implementing SSL in IIS and Apache. Attacks on HTTPS flows with sslstrip and sslsnif.

7) System and software configuration

- Default configuration, the major risk.
- Rules to follow when installing an operating system.
- Linux or Windows. Apache or IIS?
- How do you configure Apache and IIS for optimal security?
- Middleware and the database. VDSs (Vulnerability Detection Systems).
Hands-on work : Web front-end security procedure (Apache or IIS).

8) Principle of secure development

- Development security: What's the right budget?
- Security in the development cycle.
- The role of client-side code: Security or ergonomics?
- Checking data sent by the client.
- Fighting buffer overflow attacks.
- Development rules to follow.
- How to fight residual risks: Headers, poorly formed URL, cookie poisoning, etc. ?

9) User authentication

- Authentication via HTTP: Basic Authentication and Digest Authentication or application-based authentication (HTML form).
- Strong authentication: X509 client certificate, Token SecurID, Mobilegov Digital DNA, etc.
- Other software authentication techniques: CAPTCHA, Keypass, etc.
- Password attacks: Sniffing, brute force, phishing, keyloggers, etc.
- Attack on session numbers (session hijacking) or on cookies (cookie poisoning).
- Attack on HTTPS authentications (fake server, sslsniff, X509 certificate exploit, etc.).
Hands-on work : "Man in the Middle" attack on user authentication and session hijacking.

10) The "application" firewall

- Reverse-proxy and application firewall, details of the features.
- What does the application firewall add to website security?
- Inserting an application firewall into a system in production. Players on the market.
Hands-on work : Implementing an application firewall. Security policy management. Attacks and results.

DATES

REMOTE CLASS
2025 : 26 Mar, 18 Jun, 01 Oct, 31 Dec