Application Security Awareness

1 Day

Syllabus

AppSec Labs Ltd.

info@appsec-labs.com | https://appsec-labs.com | 10 HaTa'as St., Kfar Saba 44641 Israel | T: +972-9-7485005 | F: +972-9-7730595

Application Security Awareness

Seminar Description

Secure programming is the last line of defense against attacks targeted toward our systems. This seminar is an introduction to application security threats, demonstrating the security problems that exist in corporate systems with a strong emphasis on application security and secure design. The seminar covers the major security vulnerabilities including the OWASP top 10 vulnerabilities, and secure-design & coding best practices when designing and developing web applications & server based services.

This seminar main objective is raising the awareness on the problems that might occur without secure coding practices. The seminar aims to teach software engineers their important role in the corporate effort to secure its systems, while utilizing information security best practices. The student will learn about the threat landscape and the controls he should use during the software development lifecycle.

Target Audience

Members of the software development team:

- Developers
- Team leaders
- Testers / QA
- Designers & architects
- Managers

Prerequisites

Before attending this course, students should be familiar with:

- Basic knowledge in information systems
- Background knowledge in networking, the internet and the World Wide Web (WWW)
- Development background with internet applications, using at least one of those languages: .NET, Java, PHP, ASP, C/C++

Seminar topics

Application Level Attacks – Learning The Attacker's Techniques

- HTTP fundamentals
- OWASP top 10 web application risks
- Broken Authentication and Session Management
- Broken Authorization Schema
- Injections (e.g. SQL injection, command injection, etc.)
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Denial of Service (DoS)
- Browser Manipulation Attacks
- Unvalidated Redirects and Forwards
- Information Leakage
- Business Logic Attacks
- Upload File Backdoors
- Insecure Cryptographic Storage
- SSL & Digital Signatures
- Events Logging

Security Countermeasures And Best Practices

- Authentication Best Practices
- Brute Force Countermeasures
- Account Lockout vs CATPCHA
- Securing Passwords
- Authorization Best Practices
- SQL Injection Countermeasures
- Cross Site Scripting Countermeasures
- Output Encoding & Input Validation Techniques
- Cross Site Request Forgery (CSRF) Countermeasures
- Replay Attacks Countermeasures
- File Upload/Download Countermeasures
- Security Logging – What to Log and What Not to Log