Application Security for Architects

Syllabus

AppSec Labs Ltd.
info@appsec-labs.com | https://appsec-labs.com | 23 HaTa'as St., Kfar Saba 44641 Israel | T: +972-9-7485005 | F: +972-9-7730595

Application Security for Architects
2-day seminar

Seminar description

Secure programming from the design is the best defense against hackers. This seminar will demonstrate live real time hacking methods, analyze the code deficiency and insecure design that enabled the attack and most importantly, teach how to prevent such vulnerabilities by adopting secure coding best practices in order to bullet-proof your applications.

The methodology of the cycle of knowledge is as follows: understand, identify, prevent. This methodology presents the managers to keep a deeper understanding of coding vulnerabilities and security countermeasures in different areas of the software development lifecycle. The demos will enable the student to get a firsthand experience of the hackers' world and what could be done to stop him.

Target audience

Members of the software development team:

- Designers & Architects
- Developers

Prerequisites

Before attending this seminar, students should be familiar with:

- Basic knowledge of Applications & Programming concepts
- Basic knowledge in networking, the internet and information systems

Seminar topics

Day 1:

Introduction to Application Security

- Why do we need information security?
- Motivation & costs
- What is Application Security?
- Common application threats
- The attacker
- Real Incidents
- Growing awareness of security
- Fraud
- Privacy standards and Regulations

Application Level Threats

- Authentication
- Authorization
- Input Validation
- Output Encoding
- Browser Manipulation
- Business Logic
- Exception Management
- File Handling
- Data Confidentiality & Integrity
- Security Logging
- Desktop Applications

Day 2:

Secure Architecture

- Components and Layers
- Network separation
- Least access / Least use
- OS isolation
- Monitoring
- Encrypted data transfer
- Common security principles
- Segmentation
- Layered security
- Input validation
- Authentication & Authorization
- Fail security
- Configuration management
- Data protection
- Security auditing

Secure Design

- Establishing security requirements
- Attack surface reduction
- Threat Modeling
- Mitigation strategies
- SDL Developer Starter Kit

SDL overview

- SDL objective
- Waterfall VS. Agile SDL
- Security risk assessment
- Privacy and security
- Code Review
- Dynamic analysis
- Security Bug-bar
- Incident-response plan
- SDL in the cloud

Designing Secure Crypto Mechanism

- Introduction to cryptography
- Symmetric cryptography
- Asymmetric cryptography
- Hash and H-MAC
- Digital signatures
- Key derivation functions