Training: SCADEMY

CL-OJA OWASP Top 10, Java Secure Coding Follow Up

TRAINING GOALS:

This course is the next step for our participants, who completed our OWASP Top 10, Java Secure Coding Fundamentals course. This is a follow up training, meaning that in order to attend this, everyone must already have the knowledge that is covered in the Fundamentals.

This course enables our participants to gain a deeper knowledge in the field, because here we emphasize the Java-specific aspects of secure coding instead of the general vulnerabilities.

At the end of the training everyone has the possibility to take an exam, where they are able to measure their level of the gained knowledge.

Participants attending this course will:

- Learn client-side vulnerabilities and secure coding practices
- Have a practical understanding of cryptography
- Learn to use various security features of the Java development environment

Audience:

- Web developers

CONSPECT:

- Client-side security
  - JavaScript security
  - Same Origin Policy
  - Simple requests
  - Preflight requests
  - Exercise – Client-side authentication
  - Client-side authentication and password management
  - Protecting JavaScript code
  - Clickjacking
    - Clickjacking
    - Exercise – IFrame, Where is My Car?

        - Protection against Clickjacking
        - Anti frame-busting – dismissing protection scripts
        - Protection against busting frame busting
    - AJAX security
        - XSS in AJAX
        - Script injection attack in AJAX
        - Exercise – XSS in AJAX
        - XSS protection in AJAX
        - Exercise CSRF in AJAX – JavaScript hijacking
        - CSRF protection in AJAX
- Practical cryptography
    - Rule #1 of implementing cryptography
    - Cryptosystems
        - Elements of a cryptosystem
        - Java Cryptography Architecture / Extension (JCA/JCE)
        - Using Cryptographic Service Providers
        - FIPS 140-2
    - Symmetric-key cryptography
        - Providing confidentiality with symmetric cryptography
        - Symmetric encryption algorithms
        - Modes of operation
        - Private (symmetric) key cryptography in Java
    - Other cryptographic algorithms
        - Hash or message digest
        - Hash algorithms
        - SHAttered
        - Hashing in Java: MessageDigest class
        - MAC and password-based encryption in Java: Mac class
        - Message Authentication Code (MAC)
        - Providing integrity and authenticity with a symmetric key
        - Random number generation
            - Random numbers and cryptography
            - Cryptographically-strong PRNGs
            - Weak and strong PRNGs in Java
            - Hardware-based TRNGs
            - Exercise RandomTest

      - Using random numbers in Java – spot the bug!
  - Asymmetric (public-key) cryptography
    - Providing confidentiality with public-key encryption
    - Rule of thumb – possession of private key
    - The RSA algorithm
      - Introduction to RSA algorithm
      - Encrypting with RSA
      - Combining symmetric and asymmetric algorithms
      - Digital signing with RSA
      - Exercise Sign
  - Public Key Infrastructure (PKI)
    - Root of Trust Concept
      - Man-in-the-Middle (MitM) attack
      - Digital certificates against MitM attack
      - Certificate Authorities in Public Key Infrastructure
      - X.509 digital certificate
      - The Java Keystore (JKS)
      - Java Certification Path (CertPath)
- Secure communication in Java
  - SSL and TLS
  - Usage options
  - Security services of TLS
  - SSL/TLS handshake
- Java security services
  - Java security services – architecture

REQUIREMENTS:

General Java development

Difficulty level

🟨🟨🟨⬜⬜⬜

CERTIFICATE:

The participants will obtain certificates signed by SCADEMY (course completion).

TRAINER:

Authorized SCADEMY Trainer

ADDITIONAL INFORMATION:

Related courses:

- CL-JSM Java and Web application security master course
- CL-WTS Web application security testing
- CL-WSC - Web application security

Note: Training come with a number of easy-to-understand exercises providing live hacking fun. By accomplishing these exercises with the lead of the trainer, participants can analyze vulnerable code snippets and commit attacks against them in order to fully understand the root causes of certain security problems. All exercises are prepared in a plug-and-play manner by using a pre-set desktop virtual machine, which provides a uniform development environment.