Training: SCADEMY
CL-OJF OWASP Top 10, Java Secure Coding Fundamentals

TRAINING GOALS:

Writing web applications in Java can be rather complex – reasons range from dealing with legacy technologies or under documented third-party components to sharp deadlines and code maintainability. Yet, beyond all that, what if we told you that attackers were trying to break into your code right now? How likely would they be to succeed?

This course will change the way you look at your Java code. We'll teach you the common weaknesses and their consequences that can allow hackers to attack your system, and – more importantly – best practices you can apply to protect yourself. We cover typical Web vulnerabilities with a focus on how they affect Java web apps on the entire stack – from the Java runtime environment to modern AJAX and HTML5-based frontends. In addition, we discuss the security aspects of the Java platform itself as well as typical Java programming mistakes you need to be aware of. We present the entire course through live practical exercises to keep it engaging and fun.

Writing secure code will give you a distinct edge over your competitors. It is your choice to be ahead of the pack – take a step and be a game-changer in the fight against cybercrime.

Participants attending this course will:

- Understand basic concepts of security, IT security and secure coding
- Learn Web vulnerabilities beyond OWASP Top Ten and know how to avoid them
- Learn about XML security
- Learn client-side vulnerabilities and secure coding practices
- Learn about typical coding mistakes and how to avoid them
- Get information about some recent vulnerabilities in the Java framework
- Get sources and further readings on secure coding practices

Audience:

- Web developers

CONSPECT:

- IT security and secure coding
  - Nature of security

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- What is risk?
- IT security vs. secure coding
- From vulnerabilities to botnets and cybercrime
  - Nature of security flaws
  - From an infected computer to targeted attacks
  - The Seven Pernicious Kingdoms
  - OWASP Top Ten 2017

- Web application security
  - Injection
    - Injection principles
    - SQL injection
      - Exercise – SQL injection
      - Typical SQL Injection attack methods
      - Blind and time-based SQL injection
      - SQL injection protection methods
      - Effect of data storage frameworks on SQL injection
  - Other injection flaws
    - Command injection
    - Case study – ImageMagick
  - Broken authentication
    - Session handling threats
    - Session handling best practices
    - Session handling in Java
    - Setting cookie attributes – best practices
    - Cross site request forgery (CSRF)
      - CSRF prevention
      - CSRF prevention in Java frameworks
  - XML external entity (XXE)
    - XML Entity introduction
    - XML external entity attack (XXE) – resource inclusion
    - XML external entity attack – URL invocation
    - XML external entity attack – parameter entities
    - Exercise – XXE attack
    - Preventing entity-related attacks
    - Case study – XXE in Google Toolbar
  - Broken access control

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Typical access control weaknesses
- Insecure direct object reference (IDOR)
- Exercise – Insecure direct object reference
- Protection against IDOR
- Case study – Facebook Notes

- Cross-Site Scripting (XSS)
  - Persistent XSS
  - Reflected XSS
  - DOM-based XSS
  - Exercise – Cross Site Scripting
  - XSS prevention
  - XSS prevention tools in Java and JSP
- HTML5 security
  - New XSS possibilities in HTML5
  - HTML5 clickjacking attack – text field injection
  - HTML5 clickjacking – content extraction
  - Form tampering
  - Exercise – Form tampering
  - Cross-origin requests
  - HTML proxy with cross-origin request
  - Exercise – Client side include
- Insecure deserialization
  - Serialization and deserialization basics
  - Security challenges of deserialization
  - Deserialization in Java
  - Denial-of-service via Java deserialization
  - From deserialization to code execution
  - POP payload targeting InvokerTransformer (Java)
  - Real-world Java deserialization vulnerabilities
  - Issues with alternative Java object deserialization methods
  - Secure deserialization with FST
  - Secure deserialization with Kryo
  - Issues with deserialization – JSON
  - Best practices against deserialization vulnerabilities
  - Case study – XML deserialization in Apache Struts leading to RCE
    - CVE-2017-9805 – Apache Struts RCE when deserializing XML

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Example XML triggering the RCE
- Using components with known vulnerabilities
  - Vulnerability attributes
  - Common Vulnerability Scoring System – CVSS
- Insufficient logging and monitoring
  - Detection and response
  - Logging and log analysis
  - Intrusion detection systems and Web application firewalls

- Common coding errors and vulnerabilities
  - Input validation
    - Input validation concepts
    - Integer problems
      - Representation of negative integers
      - Integer overflow
      - Exercise IntOverflow
      - What is the value of Math.abs(Integer.MIN_VALUE)?
      - Integer problem – best practices
    - Path traversal vulnerability
      - Path traversal – weak protections
      - Path traversal – best practices
    - Unvalidated redirects and forwards
    - Log forging
      - Some other typical problems with log files
  - Improper use of security features
    - Typical problems related to the use of security features
    - Password management
      - Exercise – Weakness of hashed passwords
      - Password management and storage
      - Special purpose hash algorithms for password storage
      - Argon2 and PBKDF2 implementations in Java
      - bcrypt and scrypt implementations in Java
      - Case study – the Ashley Madison data breach
      - Typical mistakes in password management
      - Exercise – Hard coded passwords
    - Accessibility modifiers
      - Accessing private fields with reflection in Java

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Exercise Reflection – Accessing private fields with reflection
- Exercise ScademyPay – Integrity protection weakness
- Improper error and exception handling
  - Typical problems with error and exception handling
  - Empty catch block
  - Overly broad throws
  - Overly broad catch
  - Using multi-catch
  - Returning from finally block – spot the bug!
  - Catching NullPointerException
  - Exception handling – spot the bug!
  - Exercise ScademyPay – Error handling
- Code quality problems
  - Dangers arising from poor code quality
  - Poor code quality – spot the bug!
  - Unreleased resources
  - Private arrays – spot the bug!
  - Private arrays – typed field returned from a public method
  - Exercise Object Hijack
  - Public method without final – object hijacking
  - Serialization – spot the bug!
  - Exercise Serializable Sensitive
  - Immutable String – spot the bug!
  - Exercise Immutable Strings
  - Immutability and security
- Principles of security and secure coding
  - Matt Bishop’s principles of robust programming
  - The security principles of Saltzer and Schroeder
- Knowledge sources
  - Secure coding sources – a starter kit
  - Vulnerability databases
  - Java secure coding sources
  - Recommended books – Java

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

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

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.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007