Training: SCADEMY
CL-WSM Web application security master course

TRAINING GOALS:

As a developer, your duty is to write bulletproof code. However...

What if we told you that despite all of your efforts, the code you have been writing your entire career is full of weaknesses you never knew existed? What if, as you are reading this, hackers were trying to break into your code? How likely would they be to succeed?

This advanced course will change the way you look at code. A hands-on training during which we will teach you all of the attackers' tricks and how to mitigate them, leaving you with no other feeling than the desire to know more.

It is your choice to be ahead of the pack, and be seen as 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
- Understand Content Security Policy
- Learn client-side vulnerabilities and secure coding practices
- Learn about denial of service attacks and protections
- Understand security concepts of Web services
- Learn about JSON security
- Have a practical understanding of cryptography
- Understand essential security protocols
- Understand some recent attacks against cryptosystems
- Learn about typical coding mistakes and how to avoid them
- Get information about some recent vulnerabilities in the Java framework
- Understand security considerations in the SDLC
- Understand security testing approaches and methodologies
- Get practical knowledge in using security testing techniques and tools
- Learn how to set up and operate the deployment environment securely
- Get sources and further readings on secure coding practices

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

Audience:

Web application developers, software architects and testers

CONSPECT:

- IT security and secure coding
  - Nature of security
  - What is risk?
  - IT security vs. secure coding
  - From vulnerabilities to botnets and cybercrime
    - Nature of security flaws
    - Reasons of difficulty
    - From an infected computer to targeted attacks
  - Classification of security flaws
    - Landwehr's taxonomy
    - The Seven Pernicious Kingdoms
    - OWASP Top Ten 2017
- Web application security (OWASP Top Ten 2017)
  - A1 - 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
  - A2 - 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- CSRF prevention in Java frameworks
- A3 - Sensitive data exposure
  - Sensitive data exposure
  - Transport layer security
    - Enforcing HTTPS
- A4 - 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
- A5 - Broken access control
  - Typical access control weaknesses
  - Insecure direct object reference (IDOR)
  - Exercise – Insecure direct object reference
  - Protection against IDOR
  - Case study – Facebook Notes
- A6 - Security misconfiguration
  - Security misconfiguration
  - Configuring the environment
  - Insecure file uploads
  - Exercise – Uploading executable files
  - Filtering file uploads – validation and configuration
- Web application security (OWASP Top Ten 2017)
  - A7 - Cross-Site Scripting (XSS)
    - Persistent XSS
    - Reflected XSS
    - DOM-based XSS
    - Exercise – Cross Site Scripting
    - XSS prevention
    - XSS prevention tools in Java and JSP
  - A8 - Insecure deserialization
    - Serialization and deserialization basics
    - Security challenges of deserialization

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- 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 deserialization – JSON
- Best practices against deserialization vulnerabilities

- A9 - Using components with known vulnerabilities
- A10 - Insufficient logging and monitoring
  - Detection and response
  - Logging and log analysis

- Content security policy
  - Directives
  - Sources
  - Extensions
- 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- HTML5 security
  - New XSS possibilities in HTML5
  - Client-side persistent data storage
  - 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
- Denial of service
  - DoS introduction
  - Asymmetric DoS
  - Regular expression DoS (ReDoS)
    - Exercise ReDoS
    - ReDoS mitigation
    - Case study – ReDos in Stack Exchange
  - Hashtable collision attack
    - Using hashtables to store data
    - Hashtable collision
    - Hashtable collision in Java
  - XML security
    - Introduction
    - XML parsing
  - XML injection
    - (Ab)using CDATA to store XSS payload in XML
    - Exercise – XML injection
    - Protection through sanitization and XML validation
    - XML bomb
    - Exercise – XML bomb
  - JSON security
    - Embedding JSON server-side
    - JSON injection
    - JSON hijacking
    - Case study – XSS via spoofed JSON element
- Practical cryptography

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- Rule #1 of implementing cryptography
- Cryptosystems
  - Elements of a cryptosystem
  - Java Cryptography Architecture / Extension (JCA/JCE)
  - Using Cryptographic Service Providers
- 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)
  - Man-in-the-Middle (MitM) attack

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- Digital certificates against MitM attack
- Certificate Authorities in Public Key Infrastructure
- X.509 digital certificate
- The Java Keystore (JKS)
- Java Certification Path (CertPath)

- Web of Trust (WoT)
  - Web of Trust (WoT) – introduction
  - WoT example
  - Challenges of Web of Trust

- Security protocols
  - The TLS protocol
    - SSL and TLS
    - Usage options
    - Security services of TLS
    - SSL/TLS handshake
    - Java Secure Socket Extension (JSSE)
  - Protocol-level vulnerabilities
    - BEAST
    - FREAK
    - FREAK – attack against SSL/TLS
    - Logjam attack
  - Padding oracle attacks
    - Adaptive chosen-ciphertext attacks
    - Padding oracle attack
    - CBC decryption
    - Padding oracle example
    - Lucky Thirteen
    - POODLE

- 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)?

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- 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

- Common coding errors and vulnerabilities
  - 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
      - Brute forcing
      - 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
    - Insufficient anti-automation
      - Captcha
      - Captcha weaknesses
    - Accessibility modifiers
      - Accessing private fields with reflection in Java
      - 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!

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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 ScademyPay – Error handling
    - Time and state problems
        - Time and state related problems
        - Concurrency – spot the bug!
        - Calling Thread.run()
        - Race condition in servlets – spot the bug!
        - Race condition – spot the bug!
        - ArrayList vs Vector
    - 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
- Security in the software development lifecycle
    - Building Security In Maturity Model (BSIMM)
    - Software Assurance Maturity Model (SAMM)
    - Microsoft Security Development Lifecycle (SDL)
        - Microsoft Security Development Lifecycle (SDL)
        - Pre-SDL Requirements: Security Training
        - Phase One: Requirements
        - Phase Two: Design
        - Phase Three: Implementation
        - Phase Four: Verification
        - Phase Five: Release
        - Post-SDL Requirement: Response
        - SDL Process Guidance for LOB Apps
        - SDL Guidance for Agile Methodologies
- Security testing

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- Functional testing vs. security testing
- Security vulnerabilities
- Prioritization – risk analysis
- Security assessments in various SDLC phases

- Security testing methodology
  - Steps of test planning (risk analysis)
  - Scoping and information gathering
    - Stakeholders
    - Assets
    - Exercise – Identifying assets
    - Security objectives for testing
    - Exercise – Defining security objectives
  - Threat modeling
    - Attacker profiles
    - Threat modeling
    - Threat modeling based on attack trees
    - Exercise – Craft an attack tree
    - Threat modeling based on misuse/abuse cases
    - Misuse/abuse cases – a simple example
    - Exercise – Craft a misuse case
    - SDL threat modeling
    - The STRIDE threat categories
    - Diagramming – elements of a DFD
    - Data flow diagram – example
    - Threat enumeration – mapping STRIDE to DFD elements
    - Risk analysis – classification of threats
    - The DREAD risk assessment model
    - Exercise – Risk analysis
    - Mitigation concepts
    - Standard mitigation techniques of MS SDL

- Security testing techniques and tools
  - General testing approaches
  - Design review
    - Assessment of security requirements
    - Identifying security-critical aspects – hotspots
  - Source code review

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- Code review for software security
- Taint analysis
- Heuristic-based
- Static code analysis
  - Static code analysis
  - Exercise – Using static code analysis tools

- Testing the implementation
  - Manual vs. automated security testing
  - Penetration testing
  - Stress tests
  - Proxy servers and sniffers
    - Testing with proxies and sniffers
    - Packet analyzers and proxies
    - Exercise – Testing with proxy
  - Web vulnerability scanners
    - Exercise – Using a vulnerability scanner
- Deployment environment
  - Assessing the environment
  - Configuration management
    - Configuration management
  - Hardening
    - Hardening
    - Network-level hardening
    - Server hardening – principle of least privilege
    - Hardening the deployment – server administration
    - Hardening the deployment – access control
  - Patch and vulnerability management
    - Patch management
    - Vulnerability repositories
    - Vulnerability attributes
    - Common Vulnerability Scoring System – CVSS
    - Vulnerability management software
    - Exercise – checking for vulnerable packages
- Principles of security and secure coding
  - Matt Bishop’s principles of robust programming
  - The security principles of Saltzer and Schroeder

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- Knowledge sources
  - Secure coding sources – a starter kit
  - Vulnerability databases
  - Java secure coding sources
  - Recommended books – Java

REQUIREMENTS:

General Web application development

Difficulty level

CERTIFICATE:

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

TRAINER:

Authorized SCADEMY Trainer

ADDITIONAL INFORMATION:

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.

SCADEMY together with online application security educational platform AVATAO (more about AVATAO www.avatao.com) for each of participant SCADEMYs authorized training adds the 30 days business AVATAO trial holds the following package:

- 30-day customized free trial

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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