Training: SCADEMY
CL-IFINT Secure coding master course for banking and finance

TRAINING GOALS:

"Money makes the world go round...." – remember? And yes: it is your responsibility to secure all that. As a fintech company you have to take up the challenge, and beat the bad guys with bomb-proof, secure applications!

If there is a domain where security is critical, it is definitely fintech. Vulnerability is not an option if you want to stay a trusted and reliable vendor with systems and applications that certainly comply with PCI-DSS requirements. You need devoted secure coders with high-level professional attitude and developers eager to fight all coding problems: yes, you need a skilled team of software engineers.

Want to know why? Just for the record: even though IT security best practices are widely available, 90% of security incidents stem from common vulnerabilities as a result of ignorance and malpractice. So, you better keep loaded in all possible ways with up to date knowledge about secure coding – unless you *wanna cry*!

We offer a training program exclusively targeting engineers developing applications for the banking and finance sector. Our dedicated trainers share their experience and expertise through hands-on labs, and give real-life case studies from the banking industry – engaging participants in live hacking fun to reveal all consequences of insecure coding.

Participants attending this course will:

- Understand basic concepts of security, IT security and secure coding
- Understand special threats in the banking and finance sector
- Understand regulations and standards
- 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
- Have a practical understanding of cryptography
- Understand the requirements of secure communication
- Understand essential security protocols
- Understand some recent attacks against cryptosystems
- Understand security concepts of Web services
- Learn about JSON security
- Learn about typical coding mistakes and how to avoid them

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

- Get information about some recent vulnerabilities in the Java framework
- Learn about denial of service attacks and protections
- Get practical knowledge in using security testing techniques and tools
- Get sources and further readings on secure coding practices

Audience:

- Developers working in the banking and finance (fintech) sector

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
    - CWE/SANS top 25 most dangerous software errors
    - SEI CERT secure coding standards
- Special threats in the banking and finance sector
  - Banking and finance threats – trends
  - Banking and finance threats – some numbers
  - Attacker profiles
  - Most significant targets
  - Industry and regulatory response to threats
  - Attacker tools and vectors
- Regulations and standards
  - The fintech cybersecurity regulatory / compliance landscape
  - Important organizations and regulations from an IT standpoint
  - Managing sensitive data
  - Breach disclosure obligations

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

- PCI DSS compliance
  - PCI DSS at a glance
  - The main assets protected by PCI-DSS
  - Requirements
    - Requirement 6 – Develop and maintain secure systems and applications
    - 6.1 – Identifying vulnerabilities, risk management
    - 6.2 – Patching
    - 6.3 – Secure software development
    - 6.4 – Policies and procedures
    - 6.5 – Train developers in secure coding best practices
    - 6.6 – Security assessment and attack detection
    - 6.7 – Documentation and enforcement
- 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
    - Setting cookie attributes – best practices
    - Case study – Authentication issues in Danish online banking
      - Danske Bank website debug mode information leak
      - Danske Bank session leakage and potential hijack vulnerability
    - Cross site request forgery (CSRF)
      - Login CSRF
      - CSRF prevention
- Web application security (OWASP Top Ten 2017)
  - A3 - Sensitive data exposure

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

- Sensitive data exposure
- Case study – Distributed guessing attack against payment cards
  - Information leakage weaknesses in online payment systems
  - Practical guessing attack
  - Real-world exploitation and countermeasures
- 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
  - Case study – XXE in Google Toolbar
  - Case study – XXE in TGI Friday's ordering system
    - Identifying the vulnerability: JSON input processed as XML
- 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
  - Exercise – Authorization bypass
- A6 - Security misconfiguration
  - Configuring the environment
  - Insecure file uploads
  - Exercise – Uploading executable files
  - Filtering file uploads – validation and configuration
- A7 - Cross-Site Scripting (XSS)
  - Persistent XSS
  - Reflected XSS
  - DOM-based XSS
  - Exercise – Cross Site Scripting
  - Exploitation: CSS injection
  - Exploitation: injecting the tag
  - Exercise – HTML injection with base tag

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

- XSS prevention
- A8 - Insecure deserialization
  - Deserialization basics
  - Security challenges of deserialization
  - Issues with deserialization – JSON
- A9 - Using components with known vulnerabilities
  - Vulnerability attributes
  - Common Vulnerability Scoring System – CVSS
- A10 - Insufficient logging and monitoring
  - Detection and response
  - Logging and log analysis
  - Intrusion detection systems and Web application firewalls

- Client-side security
  - JavaScript security
  - Same Origin Policy
  - Cross Origin Resource Sharing (CORS)
  - Exercise – Client-side authentication
  - Client-side authentication and password management
  - Protecting JavaScript code
  - Clickjacking
    - Exercise – Do you Like me?
    - 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
  - HTML5 security
    - New XSS possibilities in HTML5
    - HTML5 clickjacking attack – text field injection
    - HTML5 clickjacking – content extraction
    - Form tampering

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 – Form tampering
- Cross-origin requests
- HTML proxy with cross-origin request
- Exercise – Client side include

- Security architecture
  - (platform and technology dependent topics)
  - Application level access control
    - (permissions, sandboxing)
  - User level access control
    - Authentication
    - Authorization

- Requirements of secure communication
  - Security levels
  - Secure acknowledgment
    - Malicious message absorption
      - Feasibility of secure acknowledgment
      - The solution: Clearing Centers
    - Inadvertent message loss
  - Integrity
    - Error detection - Inadvertent message distortion (noise)
      - Modeling message distortion
      - Error detection and correction codes
    - Authenticity - Malicious message manipulation
      - Modeling message manipulation
      - Practical integrity protection (detection)
    - Non-repudiation
    - Summary
      - Detecting integrity violation
  - Confidentiality
    - Model of encrypted communication
    - Encryption methods in practice
    - Strength of encryption algorithms
  - Remote identification
    - Requirements of remote identification
  - Anonymity and traffic analysis
    - Model of anonymous communication

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

- Traffic analysis
- Theoretically strong protection against traffic analysis
- Practical protection against traffic analysis

- Summary
  - Relationship between the requirements

- Practical cryptography
  - Rule #1 of implementing cryptography
  - Cryptosystems
    - Elements of a cryptosystem
  - Symmetric-key cryptography
    - Providing confidentiality with symmetric cryptography
    - Symmetric encryption algorithms
    - Modes of operation
  - Other cryptographic algorithms
    - Hash or message digest
    - Hash algorithms
    - SHAttered
    - Message Authentication Code (MAC)
    - Providing integrity and authenticity with a symmetric key
    - Random numbers and cryptography
    - Cryptographically-strong PRNGs
    - Hardware-based TRNGs
  - 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
  - Public Key Infrastructure (PKI)
    - Man-in-the-Middle (MitM) attack
    - Digital certificates against MitM attack
    - Certificate Authorities in Public Key Infrastructure
    - X.509 digital certificate
- Crypto libraries and APIs

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

- (platform and technology dependent topics)
- Security protocols
  - SSL/TLS protocols
    - Security services
    - SSL/TLS handshake
  - Protocol-level vulnerabilities
    - BEAST
  - Padding oracle attacks
    - Adaptive chosen-ciphertext attacks
    - Padding oracle attack
    - CBC decryption
    - Padding oracle example
    - POODLE
- Input validation
  - Input validation concepts
  - Integer problems
    - Representation of negative integers
    - Integer overflow
    - Integer problem – best practices
    - Case study – Integer overflow in the Stockholm Stock Exchange
      - Integer wraparound problem when purchasing stocks
    - Path traversal vulnerability
      - Path traversal – best practices
      - Case study – Insufficient URL validation in LastPass
    - Unvalidated redirects and forwards
      - Log forging
        - Some other typical problems with log files
      - (some additional platform and technology dependent topics)
- Security of Web services
  - Securing web services – two general approaches
  - SOAP - Simple Object Access Protocol
  - Security of RESTful web services
    - Authenticating users in RESTful web services
    - Authentication with JSON Web Tokens (JWT)
    - Authorization with REST
    - Vulnerabilities in connection with REST

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

- 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
  - Introduction
  - JSON parsing
  - Embedding JSON server-side
  - JSON injection
  - JSON hijacking
  - Case study – XSS via spoofed JSON element
- Improper use of security features
  - Typical problems related to the use of security features
  - Insecure randomness
    - Case study – Equifax account freeze PIN code generation
    - Case study – Tesco Bank fraud
      - Fraud exploiting deterministic card number generation
  - Password management
    - Exercise – Weakness of hashed passwords
    - Password management and storage
    - Special purpose hash algorithms for password storage
    - Case study – the Ashley Madison data breach
      - The loginkey token
      - Revealing the passwords with brute forcing
    - Typical mistakes in password management
  - Case study – Equifax password management issues
  - (some additional platform and technology dependent topics)
- Object-relational mapping (ORM) security
  - (platform and technology dependent topics)
- Improper error and exception handling
  - Typical problems with error and exception handling

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

- Time and state problems
  - (platform and technology dependent topics)
- Code quality problems
  - (platform and technology dependent topics)
- Denial of service
  - DoS introduction
  - Asymmetric DoS
  - SSL/TLS renegotiation DoS
  - Case study – ReDos in Stack Exchange
  - Hashtable collision attack
    - Using hashtables to store inputs
    - Hashtable collision
- Security testing techniques and tools
  - General testing approaches
  - Source code review
    - Code review for software security
    - Taint analysis
    - Heuristic-based
    - Static code analysis
  - Testing the implementation
    - Dynamic security testing
    - Manual vs. automated security testing
    - Penetration testing
    - Stress tests
    - Fuzzing
      - Automated security testing - fuzzing
      - Challenges of fuzzing
    - Proxy servers and sniffers
      - Testing with proxies and sniffers
      - Packet analyzers and proxies
      - Exercise – Testing with proxy
      - Proxying HTTPS traffic
      - Case study – The Lenovo Superfish incident
    - Web vulnerability scanners
    - Exercise – Using a vulnerability scanner
    - SQL injection tools

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 – Using SQL injection tools
    - Principles of security and secure coding
        - Matt Bishop’s principles of robust programming
        - The security principles of Saltzer and Schroeder
        - SEI Cert top 10 secure coding practices
    - Knowledge sources
        - Secure coding sources – a starter kit
        - Vulnerability databases

REQUIREMENTS:

Advanced desktop and 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 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