Training: SCADEMY
CL-CLS Application security in the cloud

TRAINING GOALS:

Migrating to the cloud introduces immense benefits for companies and individuals in terms of efficiency and costs. With respect to security, the effects are quite diverse, but it is a common perception that using cloud services impacts security in a positive manner. Opinions, however, diverge many times even on defining who is responsible for ensuring the security of cloud resources.

Covering IaaS, PaaS and SaaS, first the security of the infrastructure is discussed: hardening and configuration issues as well as various solutions for authentication and authorization alongside identity management that should be at the core of all security architecture. This is followed by some basics regarding legal and contractual issues, namely how trust is established and governed in the cloud.

The journey through cloud security continues with understanding cloud-specific threats and the attackers' goals and motivations as well as typical attack steps taken against cloud solutions. Special focus is also given to auditing the cloud and providing security evaluation of cloud solutions on all levels, including penetration testing and vulnerability analysis.

The focus of the course is on application security issues, dealing both with data security and the security of the applications themselves. From the standpoint of application security, cloud computing security is not substantially different than general software security, and therefore basically all OWASP-enlisted vulnerabilities are relevant in this domain as well. It is the set of threats and risks that makes the difference, and thus the training is concluded with the enumeration of various cloud-specific attack vectors connected to the weaknesses discussed beforehand.

Participants attending this course will:

- Understand basic concepts of security, IT security and secure coding
- Understand major threats and risks in the cloud domain
- Learn about elementary cloud security solutions
- Understand security concepts of Web services
- Learn about XML security
- Have a practical understanding of cryptography
- Learn Web vulnerabilities beyond OWASP Top Ten and know how to avoid them
- Learn about denial of service attacks and protections
- Learn typical input validation mistakes
- Understand data security challenges in the cloud

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

- Learn about NoSQL security
- Learn about MongoDB security
- Understand the challenges of auditing and evaluating cloud systems for security
- Learn how to secure the cloud environment and infrastructure
- Learn how to set up and operate the deployment environment securely
- Get sources and further readings on secure coding practices

Audience:

Developers, architect and testers of cloud applications

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
    - The Seven Pernicious Kingdoms
    - OWASP Top Ten 2017
- loud security basics
  - Introduction to cloud security
    - What makes cloud applications different?
    - Cloud delivery models and security
    - Public and private clouds
    - Security challenges in the cloud
- Threats and risks in the clouds
  - Requirements and threats of cloud computing
    - The Jericho Cloud Cube model
    - The Jericho Cloud Cube model – Requirements specification
    - Cloud deployment models vs risks
  - Threat modeling
    - Attacker profiles
    - Main attacker profiles in the cloud
    - Threat modeling

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

- Threat modeling based on attack trees
- Threat modeling based on misuse/abuse cases
- Misuse/abuse cases – a simple example
- 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
- Standard mitigation techniques of MS SDL

- Cloud-specific threats
  - Cloud abuse by the attackers
  - Insider threats – malicious other tenants
  - Problems stemming from virtualization
  - Elevation of privilege
  - Leakage of sensitive information
    - Hard coded secrets
    - Exercise – Hard coded passwords
    - Intellectual property exposure
    - Insecure delegation

- Cloud security solutions
  - Container security
    - Virtualization techniques
    - Containers vs. VMs
    - Evolution of process isolation
    - POSIX capabilities
    - Linux Containers – LXC
    - Docker
      - Linking Docker containers
      - Docker and POSIX capabilities
      - Docker API
      - Docker container related threats
      - Docker best practices
  - XML security
    - Introduction
    - XML parsing

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

- 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

- 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 number generation
      - Random numbers and cryptography
      - Cryptographically-strong PRNGs
      - Hardware-based TRNGs
      - Testing random number generators
  - Asymmetric (public-key) cryptography
    - Providing confidentiality with public-key encryption
    - Rule of thumb – possession of private key
    - Combining symmetric and asymmetric algorithms
  - 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

- Web application security
  - Injection

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

- Injection principles
- SQL injection
  - Exercise – SQL injection
  - Typical SQL Injection attack methods
  - Blind and time-based SQL injection
  - SQL injection protection methods
  - Detecting SQL Injection
  - Detecting SQL Injection – Typical tests
  - Detecting SQL Injection – Bypass defenses
- Other injection flaws
  - Command injection
  - Detecting command injection
  - Case study – ImageMagick

- Broken authentication
  - Session handling threats
  - Session handling best practices
  - Setting cookie attributes – best practices
- 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
- Cross-Site Scripting (XSS)
  - Persistent XSS
  - Reflected XSS
  - DOM-based XSS
  - Exercise – Cross Site Scripting
  - XSS prevention
  - Detecting XSS vulnerabilities
  - Bypassing XSS filters

- Denial of service
  - DoS introduction
  - Economic Denial of Sustainability (EDoS)
  - Asymmetric DoS

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

- 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

- 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
      - Integer problem – best practices
      - Avoiding arithmetic overflow – addition
      - Avoiding arithmetic overflow – multiplication
      - Detecting arithmetic overflow in Java 8
      - Exercise – Using addExact() in Java
      - Testing for integer problems
  - Path traversal vulnerability
    - Path traversal – weak protections
    - Path traversal – best practices
  - Unvalidated redirects and forwards
  - Log forging
    - Some other typical problems with log files

- Data security in the cloud
  - Data at rest and in motion
  - Data security lifecycle in the cloud
  - Controls for data at rest
  - Controls for data in motion
  - NoSQL security
    - NoSQL introduction
    - NoSQL attack vectors

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

- NoSQL authentication issues
- MongoDB security
  - MongoDB introduction
  - MongoDB security architecture and features
    - Authentication and access control
    - Document validation in MongoDB
    - Securing MongoDB communication via TLS
    - Secure configuration and hardening
  - Typical MongoDB security issues
    - NoSQL injection in MongoDB
    - Exercise – MongoDB NoSQL injection
    - Preventing NoSQL injection – Mongoose
    - Case studies: some past MongoDB weaknesses and vulnerabilities
- Security audit in the cloud
  - Functional testing vs. security testing
  - Security vulnerabilities
  - Prioritization – risk analysis
  - Security testing techniques and tools
    - General testing approaches
- Dynamic security testing
  - Manual vs. automated security testing
  - Web vulnerability scanners
    - Exercise – Using a vulnerability scanner
    - SQL injection tools
    - Exercise – Using SQL injection tools
- Securing the cloud environment
  - Assessing the environment
  - Patch and vulnerability management
    - Patch management
    - Insecure APIs in the cloud
    - Vulnerability repositories
    - Vulnerability attributes
    - Common Vulnerability Scoring System – CVSS
    - Vulnerability management software
    - Exercise – checking for vulnerable packages
    - Case study - Shellshock

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

- Shellshock – basics of using functions in bash
- Shellshock – vulnerability in bash
- Exercise - Shellshock
- Shellshock fix and counterattacks
- Exercise – Command override with environment variables

- Knowledge sources
  - Secure coding sources – a starter kit
  - Vulnerability databases
  - Recommended books – cloud security

REQUIREMENTS:

Cloud computing, software 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