Training: SCADEMY
CL-PSC Secure coding in PHP

TRAINING GOALS:

The course provides essential skills for PHP developers necessary to make their applications resistant to contemporary attacks through the Internet. Web vulnerabilities are discussed through PHP-based examples going beyond the OWASP top ten, tackling various injection attacks, script injections, attacks against session handling of PHP, insecure direct object references, issues with file upload, and many others. PHP-related vulnerabilities are introduced grouped into the standard vulnerability types of missing or improper input validation, incorrect error and exception handling, improper use of security features and time- and state-related problems. For this latter we discuss attacks like the open_basedir circumvention, denial-of-service through magic float or the hash table collision attack. In all cases participants will get familiar with the most important techniques and functions to be used to mitigate the enlisted risks.

A special focus is given to client-side security tackling security issues of JavaScript, Ajax and HTML5. A number of security-related extensions to PHP are introduced like hash, mcrypt and OpenSSL for cryptography, or Ctype, ext/filter and HTML Purifier for input validation. Hardening best practices are given in connection with PHP configuration (setting php.ini), Apache and the server in general. Finally, an overview is given to various security testing tools and techniques which developers and testers can use, including security scanners, penetration testing and exploit packs, sniffers, proxy servers, fuzzing tools and static source code analyzers.

Both the introduction of vulnerabilities and the configuration practices are supported by a number of hands-on exercises demonstrating the consequences of successful attacks, showing how to apply mitigation techniques and introducing the use of various extensions and tools.

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 to use various security features of PHP
- Have a practical understanding of cryptography
- Learn how to set up and operate the deployment environment securely
- Learn about denial of service attacks and protections
- Learn about typical coding mistakes and how to avoid them
- Be informed about recent vulnerabilities of the PHP framework

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 sources and further readings on secure coding practices

Audience:

Web developers, 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
    - 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
      - SQL injection protection in PHP
    - Other injection flaws
      - Command injection
      - Case study – ImageMagick
    - HTTP parameter pollution
      - Cookie injection / HTTP parameter pollution
  - Broken authentication
    - Session handling threats
    - Session data handling in PHP
    - Exercise – Exploiting weak session data handling
    - Session handling best practices
    - Setting cookie attributes – best practices

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

- Cross site request forgery (CSRF)
  - CSRF prevention
- 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
  - Case study – XXE in Google Toolbar
- Broken access control
  - 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
- Insecure deserialization
  - Serialization and deserialization basics
  - Security challenges of deserialization
  - Issues with deserialization – JSON

- 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 – Do you Like me?
    - Protection against Clickjacking

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

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

- 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
      - Weak PRNGs in PHP

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

- Stronger PRNGs in PHP
- Hardware-based TRNGs
- Exercise RandomTest
- Using random numbers in PHP – spot the bug!

- 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
- Cryptography in PHP
  - hash
  - mcrypt
  - openssl

- Deployment environment
  - PHP configuration
    - php.ini settings – Information disclosure
    - php.ini settings – Resource limits
    - php.ini settings – Session handling
    - php.ini settings – Other security related
    - Apache settings
- Denial of service
  - DoS introduction
  - Asymmetric DoS
  - Case study – ReDos in Stack Exchange
  - Hashtable collision attack
    - Using hashtables to store data
    - Hashtable collision
    - Hashtable collision in PHP
    - Fix for the hashtable collision attack
- Common coding errors and vulnerabilities
  - Input validation
    - Input validation concepts

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

- Path traversal vulnerability
  - Path traversal
  - Path traversal – weak protections
  - Path traversal – best practices
  - Case study – Insufficient URL validation in LastPass
- Unvalidated redirects and forwards
- Log forging
  - Some other typical problems with log files

- Input validation and escaping APIs in PHP
  - Basic input validation functions
  - Escaping in PHP
  - PHP input validation extensions
    - PHP input validation extensions
    - CType
    - ext/filter
  - Arbitrary code execution
    - Arbitrary code execution
    - Dangerous functions regarding remote code execution
    - Exercise CodeExec –Remote PHP code execution
    - Exercise: exploiting preg_replace
  - MySQL validation errors – beyond SQL Injection
    - Issues with max_packet_size
    - MySQL column truncation
    - MySQL validation best practices

- XML security
  - Introduction
  - XML parsing
  - XML injection
    - (Ab)using CDATA to store XSS payload in XML
    - Protection through sanitization and XML validation
    - XML bomb

- 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

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

- Password management and storage
- Special purpose hash algorithms for password storage
- Storing credentials for external systems in PHP
- Case study – the Ashley Madison data breach

- Improper error and exception handling
  - Typical problems with error and exception handling
  - Empty catch block
  - Overly broad catch
  - Error handling best practices
- Time and state problems
  - Concurrency and threading
  - Concurrency in PHP
  - Spot the bug – Race condition with files
  - Exercise – Race condition with files
  - Preventing file race condition
  - Double submit problem
  - PHP session handling
  - A PHP design flaw – open_basedir race condition
- Code quality
  - PHP variable initialization problems
  - PHP type comparison rules
  - Magic float
    - Magic float

- 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
  - PHP secure coding guidelines and sources – a compilation
  - Cheat sheets
  - Recommended books – PHP

REQUIREMENTS:

General Web application development

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

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