Training: SCADEMY
# CL-WTS Web application security testing

## TRAINING GOALS:

Testing plays a very important role in ensuring security and robustness of web applications. Various approaches – from high level auditing through penetration testing to ethical hacking – can be applied to find vulnerabilities of different types. However if you want to go beyond the easy-to-find low-hanging fruits, security testing should be well planned and properly executed. Remember: security testers should ideally find all bugs to protect a system, while for adversaries it is enough to find one exploitable vulnerability to penetrate into it.

Attending this course will prepare software testers to adequately plan and precisely execute security tests, select and use the most appropriate tools and techniques to find even hidden security flaws. Practical exercises will help understanding web application vulnerabilities and mitigation techniques, together with hands-on trials of various testing tools from security scanners, through sniffers, proxy servers, fuzzing tools to static source code analyzers, this course gives the essential practical skills that can be applied on the next day at the workplace.

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
- Understand security concepts of Web services
- Learn about JSON security
- Learn about denial of service attacks and protections
- Understand security testing approaches and methodologies
- Get practical knowledge in using security testing techniques and tools
- Get sources and further readings on secure coding practices

Audience:

Web application testers

## CONSPECT:

- IT security and secure coding



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

- 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
      - Detecting SQL Injection
      - Detecting SQL Injection – Typical tests
      - Detecting SQL Injection – Bypass defenses
    - Other injection flaws
      - Command injection
      - Detecting command injection
      - Case study – ImageMagick
  - A2 - Broken authentication
    - Session handling threats
    - Session handling best practices
    - Setting cookie attributes – best practices
    - Session management testing
    - Session ID predictability and randomness
    - Testing session properties
    - Cross site request forgery (CSRF)
      - Login CSRF
      - CSRF prevention



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

- Testing for CSRF vulnerabilities
- 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
  - 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
  - Testing for insecure direct object reference
  - Testing for insecure direct object references
  - Case study – Facebook Notes
- Web application security (OWASP Top Ten 2017)
  - 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
    - XSS prevention
    - Detecting XSS vulnerabilities
    - Bypassing XSS filters



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

- A8 - Insecure deserialization
  - Serialization and 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
  - 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
  - HTML5 security
    - New XSS possibilities in HTML5
    - HTML5 clickjacking attack – text field injection
    - HTML5 clickjacking – content extraction



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

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

- 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

- 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

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



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

- 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
- Testing steps
  - Deriving test cases
  - Accomplishing the tests
  - Processing test results
  - Mitigation concepts
  - Standard mitigation techniques of MS SDL
  - Review phase

- Security testing techniques and tools
  - General testing approaches
  - Source code review
    - Code review for software security
    - Taint analysis
    - Heuristic-based



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

- Static code analysis
  - Static code analysis
- 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
    - Proxying HTTPS traffic
    - Case study – The Lenovo Superfish incident
  - Web vulnerability scanners
    - Exercise – Using a vulnerability scanner
    - SQL injection tools
    - Exercise – Using SQL injection tools
- Knowledge sources
  - Secure coding sources – a starter kit
  - Vulnerability databases

## REQUIREMENTS:

General Web application development and testing

## Difficulty level



## CERTIFICATE:

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

## TRAINER:

Authorized SCADEMY Trainer



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

## 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