

Szkozenie: Capstone Courseware  
107 Java Development for Secure Systems

FORMA SZKOLENIA	MATERIAŁY SZKOLENIOWE	CENA	CZAS TRWANIA
Stacjonarne	Tradycyjne	2900 PLN NETTO*	3 dni
Stacjonarne	Tablet CTAB	3300 PLN NETTO*	3 dni
Metoda dlearning	Tradycyjne	2900 PLN NETTO*	3 dni
Metoda dlearning	Tablet CTAB	2900 PLN NETTO*	3 dni

\* (+VAT zgodnie z obowiązującą stawką w dniu wystawienia faktury)

## LOKALIZACJE

Kraków - ul. Tatarska 5, II piętro, godz. 9:00 - 16:00

Warszawa - ul. Bielska 17, godz. 9:00 - 16:00

## Cel szkolenia:

## Wersja 6.0

Kurs ukazuje szeroki zakres wyzwań i technik, które kryją się pod „**bezpieczeństwem w Java**”. Opisuje techniki dla **Java SE** oraz **Java EE**, coraz częściej jednak aplikacje EE używają technik SE, takich jak pliki polityk i uwierzytelnianie **JAAS**. Kurs poświęca czas każdej z platform, omawiając podstawy SE, takie jak AccessController, uprawnienia i polityki, oraz tradycyjne techniki EE takie jak deklaracje bezpieczeństwa sieciowego oraz model autoryzacji EJB.

Kurs kładzie nacisk na ćwiczenia praktyczne, większą część czasu kursanci spędzą na rozwiązywaniu konkretnych problemów związanych z bezpieczeństwem. Większość ćwiczeń jest zorganizowanych jako scenariusze, w których program posiada lukę bezpieczeństwa. Kursanci wpierw próbują ją wykorzystać w jakiś sposób, a następnie wyeliminować poprzez ustawienie polityki, podpisanie pliku, wyczyszczenie wystawionych części API, wymuszenie logowania etc.

Ta wersja kursu celuje w Java SE w wersji 6 i Java EE w wersji 5, jednak może być bezproblemowo zastosowana dla Java SE w wersji 5 oraz Java EE w wersji 1.4.

## Cele szkolenia:

- Projektowanie i implementacja polityk bezpieczeństwa dla aplikacji, serwerów i komponentów Java.
- Zarządzanie kluczami i certyfikatami dla aplikacji Java, oraz podpisywanie kodu źródłowego w razie potrzeby.
- Ćwiczenie bezpiecznego projektowania i programowania, oraz balansu pomiędzy funkcjonalnością a bezpieczeństwem w interfejsach użytkownika i API

- Podpisywanie i weryfikacja danych i wiadomości aplikacji przy użyciu JCA, oraz szyfrowanie/desyfrowanie za pomocą JCE.
- Wprowadzenie uwierzytelniania JASS do aplikacji
- Implementacja JAAS LoginModule do połączenia z danymi własnej aplikacji.
- Zabezpieczanie aplikacji Java EE poprzez URL oraz role, integracja uwierzytelniania JAAS
- Unikanie typowych pułapek aplikacji sieciowych w Javie, włączając SQL injection i ataki cross-site-scripting.

## Plan szkolenia:

- Java SE bezpieczeństwo
  - Holistyczne podejście do bezpieczeństwa
  - Zagrożenia dla użytkownika
  - Class Loader oraz Bytecode Verifier
  - Klasy systemowe i Core API
  - SecurityManager i AccessController
  - Uprawnienia
  - Implikacja
  - CodeSources
  - Polityki
  - Konfiguracja zabezpieczeń Java SE
  - Dynamiczne polityki
  - Akcje uprzywilejowane
- Podpisywanie kodu i zarządzanie kluczami
  - Szyfrowanie i podpis cyfrowy
  - Keystores
  - Klucze i certyfikaty
  - Urzędy certyfikacji
  - KeyStore
  - API
  - Podpisywanie JAR
  - Podpisane CodeSources
  - Additional Policy Semantics
- Praktyki bezpiecznego programowania: Java SE
  - Wstrzykiwanie kodu (Code Injection)
  - Metody i klasy finalne
  - Wzorce projektowe: singletony, metody wytórcze oraz pyłki

- Metody, kolekcje, i ukrywanie danych
- Izolowanie JAR
- Zaciemnianie kodu
- Serializacja obiektu
- Kryptografia
  - Zagrożenia dla tożsamości i prywatności
  - Rozszerzenia kryptograficzne Javy
  - Klasa Signature
  - SignedObject
  - Rozszerzenia kryptograficzne w Javie
  - SecretKey i KeyGenerator
  - Klasa Cipher
  - Niebezpieczne praktyki
  - HTTP i JSSE
- JAAS
  - Dołączana logika uwierzytelniania
  - JAAS
  - Paczki i interfejsy
  - Subjects oraz Principals
  - AND oraz OR
  - Impersonation
  - Uprawnienia JASS
  - JAAS uprawnienia
  - LoginContext oraz LoginModule
  - Konfiguracja JAAS
  - CallbackHandler i wywołania zwrotne
  - Implementacja klienta JAAS
  - Implementacja LoginModule
- Java EE bezpieczeństwo
  - Serwery Java EE jako hosty kodu
  - Konfiguracja bezpieczeństwa Tomcat
  - Deklaracja ról
  - Zabezpieczanie URL
  - Schematy uwierzytelniania HTTP
  - Zabezpieczanie EJB
  - Bezpieczeństwo programowe

- JAAS w Java EE
- Realm i LoginModules
- JAAS in Tomcat
- JACC
- Certyfikacja aplikacji Java EE
- Konfiguracja HTTPS
- Praktyki bezpiecznego programowania: Java EE
  - Zagrożenia warstwy prezentacji
  - Konta użytkowników
  - MVC i bezpieczeństwo
  - Sprawdzane danych użytkownika
  - SQL Injection
  - Cross-Site Scripting
  - Reflected XSS
  - Zwalczanie XSS
  - OWASP
  - Testy penetracyjne
  - Obsługa błędów i wyciek informacji
  - Logowanie i audytowanie

## Wymagania:

- Solidne doświadczenie w programowaniu w Java, kurs 103 [Java Programming](#) jest doskonałym przygotowaniem.
- Duże doświadczenie w programowaniu w **Java EE** nie jest wymagana, jednakże pewna wiedza o Java EE jest zalecana, kurs 108 [Overview of Java EE Development](#) jest zalecany.

## Poziom trudności



## Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat sygnowany przez firmę Capstone Courseware.

## Prowadzący:

Certyfikowany wykładowca Capstone Courseware.