

Szkozenie: Compendium CE
Bezpieczeństwo aplikacji (J2EE)

FORMA SZKOLENIA	MATERIAŁY SZKOLENIOWE	CENA	CZAS TRWANIA
Stacjonarne	Tradycyjne	4500 PLN NETTO*	2 dni
Stacjonarne	Cyfrowe	4500 PLN NETTO*	2 dni
Stacjonarne	Tablet CTAB	4900 PLN NETTO*	2 dni
Metoda dlearning	Tradycyjne	4500 PLN NETTO*	2 dni
Metoda dlearning	Cyfrowe	4500 PLN NETTO*	2 dni
Metoda dlearning	Tablet CTAB	4500 PLN NETTO*	2 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:

Szkozenie jest przeznaczone dla programistów pracujących w technologii J2EE zainteresowanych poszerzeniem swojej wiedzy dotyczącej bezpieczeństwa aplikacji webowych oraz dla osób chcących wykorzystać tą wiedzę podczas swojej pracy.

W trakcie szkolenia pojawi się dużo ćwiczeń i przykładów defektów bezpieczeństwa, opracowanych na podstawie doświadczenia trenera zdobytego podczas testowania bezpieczeństwa aplikacji. Zostaną omówione techniki i mechanizmy umożliwiające tworzenie bezpiecznych aplikacji.

Plan szkolenia:

- Wprowadzenie
 - Wprowadzenie do tematyki bezpieczeństwa sieci, systemów i aplikacji
 - Dobre praktyki, zasady i standardy
- Modelowanie zagrożeń
 - Podstawowe pojęcia
 - Istniejące podejścia
 - Warsztaty, na przykładzie aplikacji, nad którą pracuje dany zespół
- Przegląd standardów i przydatnych dokumentów
 - OWASP ASVS 2013

- OWASP TOP 10 2013
- OWASP Proactive Controls
- OWASP CheatSheets
- Security Knowledge Framework
- Komunikacja SSL/TLS
 - Wprowadzenie do PKI
 - Budowa i rodzaje certyfikatów
 - Przykłady komunikacji (analiza zapisu ruchu sieciowego SSL/TLS)
 - Bezpieczeństwo i testowanie SSL/TLS
- Bezpieczne programowanie w kontekście J2EE
 - Dostępne mechanizmy bezpieczeństwa - na poziomie kodu i konfiguracji
 - Uwierzytelnienie, sesyjność, autoryzacja
 - Kontrola dostępu do funkcji i danych - dobre praktyki, role, uprawnienia, minimalizacja powierzchni ataku
 - Walidacja danych wejściowych
 - Kodowanie na wyjściu w zależności od kontekstu (html, xml, javascript...) - automatyczne kodowanie framework-a, oraz przypadki gdy może zawieść
 - Prawidłowa konstrukcja zapytań do baz danych
 - Błędy wynikające z interpretacji Expression Language oraz deserializacji (m.in. Remote Code Execution)
 - Błędy parsowania XML (XML External Entity)
 - Prawidłowe użycie mechanizmów kryptograficznych
 - Inne częste błędy występujące w aplikacjach J2EE (m.in. błędy logiczne, nieautoryzowana zmiana wewnętrznego stanu aplikacji)
 - Bezpieczeństwo w kontekście wykorzystywanych bibliotek i frameworków (np. Struts, Spring, Wicket, JSF, ...)
 - Analiza przykładowych błędów bezpieczeństwa, z którymi spotkał się dany zespół
- Część warsztatowa (ćwiczenia, w trakcie omawiania rodzajów błędów)
- Narzędzia wspomagające i automatyzujące niektóre aspekty testów bezpieczeństwa
 - OWASP ZAP
 - OWASP Dependency Check
- Techniki utrudniania i wykrywania ataków
 - OWASP AppSensor

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat wystawiony imiennie oraz na firmę sygnowany przez Compendium Centrum Edukacyjne.

Prowadzący:

Wykładowca Compendium Centrum Edukacyjnego.