

Szkolenie: Compendium CE
Testowanie bezpieczeństwa dla specjalistów QA

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:

Szkolenie **Testowanie bezpieczeństwa dla specjalistów QA** przeznaczone jest dla osób zainteresowanych poszerzeniem swojej wiedzy o zagadnienia dotyczące **testowania bezpieczeństwa aplikacji webowych** oraz dla osób chcących wykorzystać tę wiedzę podczas swojej pracy.

W trakcie szkolenia pojawi się dużo ćwiczeń i przykładów defektów bezpieczeństwa, opracowanych na podstawie doświadczenia zdobytego przez trenera podczas testowania bezpieczeństwa aplikacji. Omówione zostaną przydatne narzędzia wykorzystywane podczas testów wraz z ich niedoskonałościami i ograniczeniami. Słuchacze poznają standardy związane z testowaniem i określaniem wymagań dotyczących **bezpieczeństwa aplikacji**.

Szkolenie to poszerzy wiedzę uczestników o podstawowe aspekty dotyczące **testowania bezpieczeństwa aplikacji webowych** oraz pozwoli na budowanie przypadków testowych związanych z bezpieczeństwem badanych aplikacji.

Szkolenie prowadzi trener posiadający kilkuletnie doświadczenie w testowaniu bezpieczeństwa aplikacji.

Plan szkolenia:

- Wprowadzenie

- Trendy
- Jak/kiedy/czemu testować bezpieczeństwo
- Realia testów bezpieczeństwa
- Modelowanie zagrożeń
 - Podstawowe pojęcia
 - Istniejące podejścia
 - Ryzyka dla aplikacji webowych i mobilnych
- Bezpieczeństwo a wymagania
 - Funkcjonalne
 - Niefunkcjonalne
- Przegląd standardów
 - OWASP ASVS 2013
 - OWASP TOP 10 2013
 - OWASP TOP 10 Mobile Risks
 - OWASP Testing Guide
- Przydatne narzędzia
 - Firebug, Web Developer, Cookie Swap
 - Fiddler
 - OWASP ZAP
 - OWASP DirBuster
- Typowe błędy
 - Walidacja danych
 - Błędy w logice biznesowej
 - Uwierzytelnianie/autoryzacja
 - XSS, SQL Injection
- Aplikacje webowe
 - Podstawy HTTP, SSL
 - Często występujące podatności
 - Techniki testowania
- Aplikacje mobilne
 - Urządzenie a API po stronie serwera
 - Mechanizmy bezpieczeństwa mobilnych systemów operacyjnych
 - Checklista dla aplikacji mobilnych
- Testy
 - Budowanie przypadków testowych
 - Automatyzacja - czy to możliwe?

- Raportowanie

Wymagania:

- Wskazane doświadczenie w testowaniu lub tworzeniu aplikacji. Mile widziana podstawowa wiedza w zakresie protokołu HTTP.

Poziom trudności



Certyfikaty:

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

Prowadzący:

Wykładowca Compendium Centrum Edukacyjnego.