Kod szkolenia: **OWASP/T**

Tytuł szkolenia: **Narzędzia OWASP dla testerów**

Dni: 2

Opis:

Adresaci szkolenia:

Testerzy bezpieczeństwa, programiści i osoby zarządzające testami pragnące poznać narzędzia OWASP i możliwości ich wykorzystania przy testach bezpieczeństwa. Wymaganiem jest znajomość podatności z listy OWASP Top Ten i podstawowych zagadnień z zakresu bezpieczeństwa aplikacji.

Cel szkolenia:

Wprowadzenie do testów bezpieczeństwa z wykorzystaniem narzędzia OWASP ZAP i innych narzędzi OWASP - konfiguracja i efektywne wykorzystanie narzędzia do prowadzenia testów aplikacji internetowych w technologiach Java i .NET z warsztatami.

Mocne strony szkolenia:

Mocną strona szkolenia jest część warsztatowa, która polega na wykorzystaniu przedstawionych modułów ZAP przy testach przykładowych aplikacji Java i .NET oraz aplikacji z maszyny wirtualnej OWASP Broken Web Apps.

- testowanie typowych podatności: Cross Site Scripting, Cross Site Request Forgery, Direct Object References za pomocą narzędzia Proxy
- wykorzystanie narzędzi Forced Browse, Spider, Fuzzer
- konfiguracja i wykorzystanie narzędzia Active Scan
- testowanie autoryzacji dostępu do funkcji za pomocą Access Control Testing
- interpretacja raportu

Wymagania

- doświadczenie w testowaniu aplikacji internetowych
- podstawowa znajomość zagadnień związanych z bezpieczeństwem aplikacji

Parametry szkolenia

2*8 godzin (2*7 godzin netto) wykładów i warsztatów (z wyraźną przewagą warsztatów).

Program szkolenia:

- co to jest OWASP i jakie są projekty OWASP: Top Ten, ASVS, narzędzia
- narzędzia udostępniane przez OWASP
    - ZAP
    - Dependency Checker
    - WebGoat
    - BWA
    - Penetration testing environment (live cd i cloud)
- moduły Owasp ZAP
    - mapowanie wykorzystania OWASP ZAP na fazy testów penetracyjnych
- wykorzystanie modułów ZAP
    - proxy
    - koder/dekoder
    - Forced browsing
    - Spider
    - Active Scan
        - analiza wyników raportu
        - dodatkowe reguły skanujące
    - Fuzzer
        - wykorzystanie fuzzera

Sages sp. z o.o., ul. Nowogrodzka 62c, 02-002 Warszawa
tel. +48 22 203 56 00 fax: +48 22 203 56 01
e-mail: biuro@sages.com.pl web: www.sages.com.pl

        - dodatkowe payloady fuzzdb
    - ZEST
        - przykłady skryptów w ZAP
    - skanowanie aplikacji wymagających uwierzytelnienia i konfiguracja różnych ról użytkowników
    - praca z aplikacjami wymagającymi uwierzytelnienia przez certyfikat klienta (SmartCard)
    - testowanie WebServices
    - Access Testing
    - generowanie raportów
    - integracja testów ZAP z narzędziem do ciągłej integracji typu Jenkins za pomocą API
- wykorzystanie pozostałych narzędzi
    - OWASP Dependency Checker - analiza komponentów