Kod szkolenia:	**OWASP**
Tytuł szkolenia:	**Zabezpieczanie aplikacji internetowych za pomocą narzędzi OWASP**
Dni:	2

Opis:

Adresaci szkolenia:

Adresatami szkolenia są programiści i administratorzy, którzy chcą zabezpieczyć aplikacje przed typowymi oraz bardziej zaawansowanymi atakami.

Cel szkolenia:

Przedstawienie metod na zabezpieczenie aplikacji internetowych przed atakami za pomocą darmowych narzędzi OWASP: AppSensor, mod_security. Prezentowane metody są przedstawione praktycznie podczas zabezpieczania przykładowych aplikacji Java i .NET w symulowanym środowisku.

Parametry szkolenia:

2 x 8 godzin (2 x 7 godzin netto) wykładów i warsztatów.

Program szkolenia:

- Wstęp: zabezpieczenia aktywne i pasywne
    - dlaczego firewall pasywny nie jest wystarczający: definicja Web Application Firewall
- Wykorzystanie mod_security i zabezpieczenia przed:
    - atakami Cross Site Scripting
    - atakami Cross Site Request Forgery
    - atakami SQL Injection

    - atakami Brute Force na przykładzie strony logowania, enumeracji stron i identyfikatorów obiektów
    - narzędziami automatycznymi
    - modyfikacją stron przez oprogramowanie malware (np. trojany bankowe typu Zeus, Banatrix)
    - zmianą adresu IP
    - logowaniem z sieci anonimizującej na przykładzie Tor
    - logowaniem z sieci o niskiej reputacji
    - wykrywanie i blokowanie spamu
    - wyciekiem danych przez wykrywanie wrażliwych danych w odpowiedziach
    - uploadem niebezpiecznych plików i wykrywanie malware we wgrywanych plikach
- wykorzystanie mod_security do aktywnej obrony:
    - dodawanie pułapek (honeytraps) do aplikacji na przykładzie fałszywego trybu administratora
    - atakowanie atakującego: BeEF
- wykorzystanie AppSensor
    - definiowanie reguł AppSensor
    - modyfikacja aplikacji w celu dodania punktów detekcji (Detection Point)