Kod szkolenia: **J/CERT**

Tytuł szkolenia: **Bezpieczny kod Java w praktyce w oparciu o wytyczne CERT i Oracle**

Dni: 3

Opis:

Adresaci szkolenia

Szkolenie adresowane jest do programistów tworzących aplikacje w środowisku Java, w szczególności rozwijających systemy o wysokich wymaganiach w kontekście bezpieczeństwa.

Cel szkolenia

Uświadomienie programistom możliwych skutków braku zachowania dobrych praktyk programowania w języku Java, w szczególności w zakresie związanym z walidacją danych wejściowych, prawidłowym wykorzystaniem mechanizmów obiektowości i dziedziczenia, wykorzystaniem odpowiednich klas, prawidłową synchronizacją pomiędzy wątkami aplikacji oraz współpracy języka Java z bibliotekami natywnymi. Omówione zostaną poszczególne zalecenia Oracle Secure Coding Guidelines for Java SE oraz SEI CERT Oracle Coding Standard for Java.

Mocne strony szkolenia

Podczas szkolenia uczestnicy:

- przekonają się o możliwych skutkach działania pozornie poprawnych implementacji,
- dla każdej z przedstawianych reguł i rekomendacji wykonają krótkie zadanie programistyczne prezentujące jej zastosowanie w praktyce,
- poznają narzędzia wspomagające walidację aplikacji w zakresie zaleceń CERT i Oracle.

Wymagania

Od uczestników szkolenia wymagana jest umiejętność programowania w języku Java. Dla programistów aplikacji internetowych zalecanym niezależnie szkoleniem jest *Zasady bezpiecznego tworzenia i utrzymywania aplikacji internetowych na platformie Java Enterprise*.

Specjalne wymagania techniczne

Uczestnicy w trakcie zajęć korzystają z komputera z systemem Linux, Windows lub macOS.

Parametry szkolenia

3 * 8 godzin (3 * 7 godzin netto) wykładów i warsztatów.

Program szkolenia:

1. Wprowadzenie
    - pułapki języka Java
    - ogólne zasady bezpiecznego programowania
    - mechanizmy bezpieczeństwa wbudowane w Java
    - zalecenia Oracle i CERT

2. Zalecenia, reguły i rekomendacje Oracle i CERT
    - przetwarzanie danych wejściowych
    - zapobieganie atakom DoS (ang. *denial of service*, odmowa usługi)
    - zapobieganie atakom wstrzyknięcia kodu (ang. *code injection*)
    - obsługa danych wrażliwych
    - deklaracja i inicjalizacja zmiennych i obiektów
    - poprawne korzystanie z mechanizmów obiektowości i dziedziczenia w Java
    - serializacja i deserializacja
    - kontrola dostępu
    - wyrażenia, typy liczbowe
    - obsługa błędów i wyjątków
    - wątki i synchronizacja, pule wątków
    - obsługa strumieni wejścia/wyjścia
    - bezpieczeństwo środowiska uruchomieniowego
    - obsługa bibliotek natywnych, Java Native Interface (JNI)
    - system Android
    - znane niedoskonałości języka Java

3. Narzędzia wspomagające
    - analiza statyczna i dynamiczna
    - przegląd wybranych narzędzi

4. Inne rekomendacje
    - specyfikacje i raporty techniczne ISO/IEC
    - MITRE CWE

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

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