SZKOLENIE ŚREDNIO ZAAWANSOWANE

Bezpieczny kod Java w oparciu o wytyczne CERT i Oracle

J/CERT

Czas trwania: 3 dni

Dobre praktyki programowania w języku Java na podstawie zaleceń CERT i Oracle

Cele szkolenia

- Umiejętność unikania typowych błędów w zakresie związanym z prawidłowym wykorzystaniem mechanizmów obiektowości i dziedziczenia, walidacją danych wejściowych oraz wykorzystaniem odpowiednich klas
- Świadomość możliwych skutków lekceważenia dobrych praktyk programowania w języku Java
- Poznanie pułapek programowania współbieżnego oraz współpracy języka Java z bibliotekami natywnymi

Zalety

- Przegląd dobrych praktyk Oracle Secure Coding Guidelines for Java SE oraz SEI CERT Oracle Coding Standard for Java na przykładzie krótkich zadań programistycznych prezentujących ich zastosowania w praktyce
- Wykorzystanie narzędzi wspomagających walidację aplikacji w zakresie zaleceń CERT i Oracle
- Poznanie możliwych skutków działania pozornie poprawnych implementacji
- Kameralne grupy - szkolenia technologiczne prowadzimy w grupach liczących do 8 osób. Pozwala to na indywidualne podejście oraz aktywizację każdego uczestnika
- Praktyka przed teorią - wszystkie szkolenia technologiczne prowadzone są w formie warsztatowej. Konieczna teoria jest wyjaśniana na przykładzie praktycznych zadań
- Konkretne umiejętności - w ramach każdego szkolenia rozwijamy praktyczne umiejętności związane z daną technologią i tematyką
- Nauka z praktykami - wszyscy trenerzy na co dzień pracują w projektach, gwarantuje to dostęp do eksperckiej wiedzy i praktycznego know-how

Dla kogo?

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

Wymagania

- Od uczestników szkolenia wymagana jest umiejętność programowania w języku Java

Program

1. Zasady bezpiecznego programowania
   a. Pułapki języka Java
   b. Mechanizmy bezpieczeństwa wbudowane w Java
   c. Zalecenia Oracle i CERT
2. Zalecenia, reguły i rekomendacje Oracle i CERT
   a. Przetwarzanie danych wejściowych
   b. Zapobieganie atakom odmowy usługi (denial of service, DoS)
   c. Zapobieganie atakom wstrzyknięcia kodu (code injection)
   d. Obsługa danych wrażliwych
   e. Deklaracja i inicjalizacja zmiennych i obiektów
   f. Poprawne korzystanie z mechanizmów obiektowości i dziedziczenia w Java
   g. Serializacja i deserializacja
   h. Kontrola dostępu
   i. Wyrażenia, typy liczbowe
   j. Obsługa błędów i wyjątków
   k. Wątki i synchronizacja, pule wątków
   l. Obsługa strumieni wejścia/wyjścia
   m. Bezpieczeństwo środowiska uruchomieniowego
   n. Obsługa bibliotek natywnych, Java Native Interface (JNI)
   o. System Android
   p. Znane niedoskonałości języka Java
3. Narzędzia wspomagające
   a. Analiza statyczna i dynamiczna
   b. Przegląd wybranych narzędzi
4. Inne rekomendacje
   a. Specyfikacje i raporty techniczne ISO/IEC
   b. MITRE CWE