„Bezpieczeństwo aplikacji webowych: JEE i .NET” – agenda szkolenia

Tematyka szkolenia obejmuje najpoważniejsze zagrożenia dla aplikacji webowych na podstawie dokumentu OWASP Top 10 (wersja 2010) i analizy rzeczywistych ataków (2011-12). Zaprezentowane zostaną praktyczne przykłady ataków na aplikacjach demonstracyjnych i zalecane metody obrony.

1. Wprowadzenie
   - zagrożenia dla aplikacji webowych
   - bezpieczeństwo w cyklu życia oprogramowania
   - prawne i etyczne aspekty testów bezpieczeństwa
2. Najpopularniejsze podatności aplikacji webowych
   - dokument OWASP Top 10
3. Otwarte przekierowania i proxy (A10)
   - phishing
   - bezpośredni dostęp do DMZ
4. Zabezpieczenia kryptograficzne
   - SSL (A9)
   - zastosowania funkcji szyfrujących i jednokierunkowych funkcji skrótu
   - przechowywanie haseł i kluczowych danych (A7)
   - szyfrowanie identyfikatorów globalnych (A4)
   - komunikacja pomiędzy aplikacjami
   - jednorazowe kody SMS/e-mail, tokeny kryptograficzne
5. Bezpośredni dostęp do danych (A8, A4)
6. Błędy konfiguracyjne
   - aktualizacje frameworka i bibliotek
   - typowe błędy
7. Uwierzytelnienie i zarządzanie sesją (A3)
   - przekazywanie identyfikatorów sesji
   - zabezpieczenia ciasteczek sesyjnych
   - same origin policy
8. Cross Site Request Forgery (CSRF, A5)
   - demonstracja ataku
   - omówienie metod obrony
   - clickjacking i aktualne ataki
9. Cross Site Scripting (XSS, A2)
   - demonstracja ataku
   - omówienie rzeczywistych ataków i metod obrony
   - trwały XSS, odbity XSS, XSS typu zerowego
10. SQL Injection (A1)
    - demonstracja ataku
    - omówienie rzeczywistych ataków i metod obrony
    - blind SQL Injection, inband SQL Injection
11. XML injection (A1)
    - demonstracja ataku
    - omówienie rzeczywistych ataków i metod obrony
    - XPath Injection, XML External Entity