Kod szkolenia: **J/SEC**

Tytuł szkolenia: **Zasady bezpiecznego tworzenia i utrzymywania aplikacji internetowych na platformie Java Enterprise**

Dni: 2

Opis:

Adresaci Szkolenia:

Szkolenie adresowane jest do programistów aplikacji internetowych, pragnących poznać zagrożenia jakie niosą różnego rodzaju błędy czy uchybienia w aplikacjach internetowych i ich otoczeniu/środowisku. Prezentowana wiedza może być przydatna dla osób odpowiedzialnych za bezpieczeństwo tworzonych lub wdrażanych aplikacji.

Cel szkolenia:

Uczestnicy dowiedzą się jak projektować i implementować bezpieczne aplikacje internetowe wykorzystujące dostępne mechanizmy najpopularniejszych technologii Javy.

W szczególności:

Uczestnicy kursu zapoznają się z najczęściej wykorzystywanymi klasami ataków na aplikacje Webowe, między innymi atakami wstrzyknięcia, XSS (Cross Site Scripting), CSRF (Cross Site Request Forgery). Każda z klas ataków zostanie szczegółowo omówiona, poczynając od omówienia błędu, poprzez sposób wykorzystania go w celu zaatakowania aplikacji, kończąc na sposobach zabezpieczenia się przed nimi. Dla najpopularniejszych technologii zostaną zaprezentowane mechanizmy umożliwiające uniknięcie poszczególnych zagrożeń. Dodatkowo uczestnicy kursu poznają narzędzia umożliwiające testowanie bezpieczeństwa aplikacji Webowych. W ramach szkolenia poruszone zostaną również aspekty konfiguracji serwera aplikacji w kontekście jej bezpiecznego udostępniania.

Mocne strony szkolenia:

Program obejmuje całościowo i wyczerpująco zagadnienia tworzenia bezpiecznych aplikacji internetowych.

Szkolenie prezentuje kluczową wiedzę do tworzenia i utrzymywania aplikacji o podwyższonych wymaganiach na bezpieczeństwo. Wiedza ta jest zwykle praktycznie niedostępna w postaci szkoleń. Uczestnicy po skończeniu szkolenia, będą mogli unikać najczęściej popełnianych błędów mogących prowadzić do udanych ataków na implementowane i wdrażane przez nich aplikacje.

Program jest ciągle uaktualniany, tak, by uwzględniać nowo powstające trendy.

Wymagania:

Od uczestników szkolenia wymagana jest umiejętność programowania w języku Java (do poznania na kursie J/JP), podstawy relacyjnych baz danych i SQL.

Zalecana jest również umiejętność tworzenia aplikacji webowych w technologiach JEE (do poznania na kursach SEAM/WEB, JEE/JSP).

Parametry szkolenia:

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

Program szkolenia:

1. Wstęp
    I. Omówienie źródeł zagrożeń dla aplikacji Webowych (błędna konfiguracja, błędy w serwerach, błędy w aplikacji…)
    II. Omówienie różnych podejścia do bezpieczeństwa/paradygmaty (Defense in depth, security by obscurity, low hanging fruits)
2. Sesja w aplikacji Webowej
    I. Sposoby realizacji sesji w aplikacjach Webowych
    II. Obsługa sesji w najpopularniejszych technologiach
    III. Atak porwania sesji (ang. session hijacking) i sposoby zabezpieczenia się
    IV. Dobre praktyki związane z obsługą sesji w aplikacjach Webowych
    V. Zapoznanie z programem WebScarab – narzędziem umożliwiającym testowanie bezpieczeństwa aplikacji
3. Ataki wstrzyknięcia (ang. injection attacks)
    I. Wprowadzenie do ataków wstrzyknięcia, powody ich występowania i metody zabezpieczenia (escapowanie oraz walidacja danych)
    II. Realizacji walidacji w najpopularniejszych technologiach
    III. Omówienie biblioteki AntiSamy, zapewniającej filtrowanie wpisywanych tagów HTML
    IV. Atak wstrzyknięcia na stronach bez pól tekstowych
    V. SQL-Injection – nie tylko „ or 1=1 ”
    VI. Nie tylko SQL-Injection (XML-Injection, X-PATH, Command Injection …)
4. Atak CSRF (ang. Cross Site Request Forgery)
    I. Omówienie idei działania ataku typu CSRF, przykład
    II. Metody zabezpieczenia się przed atakiem CSRF
5. Uwierzytelnienie i autoryzacja w aplikacjach Webowych
    I. Zapewnienie bezpiecznego sposobu uwierzytelniania
    II. Polityka dotycząca haseł (czas życia, sposób przechowywania, itp. …)
    III. Realizacja uwierzytelniania w aplikacjach opartych na Java Enterprise Edition (JAAS) oraz znanych szkieletach (Seam, Spring)
6. Obsługa błędów w aplikacjach Webowych

    I. Omówienie niebezpieczeństw związanych z nieodpowiednią obsługą błędów
        i. Co/czego nie umieszczać w komunikatach błędów
        ii. Co może zostać ujawnione w wyniku nieprawidłowej obsługi błędów
        iii. Realizacja zasady „ fail securely ”
7. Wielowątkowość
    I. Problemy związane z wielowątkowością – wyścigi oraz nadpisanie danych
    II. Cyklu życia dynamicznych stron i servletów na przykładach najpopularniejszych technologii
    III. Omówienie przykładowego ataku wykorzystującego błędne zaimplementowanie wielowątkowości
8. Bezpieczeństwo WebServices
9. Niebezpieczeństwa języka Java
10. Bezpieczna konfiguracja serwerów aplikacyjnych
11. Bezpieczna architektura dla aplikacji Webowych (wykorzystanie DMZ, filtrowanie adresów …)
12. Realizacja podmiany standardowej strony błędu
13. Inne zagadnienia związane z bezpieczeństwem
14. Zapewnienie poufności przesyłanych danych
15. Nie ufać w dobrą wolę użytkowników lub ich niewiedzę
    I. Co można znaleźć w źródłach wygenerowanych stron (debug programistów)
    II. Nie ufać w wyniki działania kodu wysyłanego do użytkownika
    III. Nie ufać w przesyłane dane od użytkownika
16. Logowanie błędów
17. Zabezpieczenia w postaci niewidocznych linków
18. Jak pisać bezpieczne aplikacje
19. Omówienie elementów służących powstawaniu bezpiecznych aplikacji
    I. Bezpieczeństwo aplikacji, jako część wymagań projektu a nie dodatek
    II. Edukacja deweloperów - WebGoat
    III. Code Review
    IV. Testowanie napisanej aplikacji (Black Box testing, Fuzzing …)
    V. Bezpieczne tworzenie aplikacji w kontekście współczesnych technologii (JEE, Seam, Spring,GWT, …)
20. Gdzie znaleźć dodatkowe informacje o częstych, znanych błędach (CERT Secure-Coding, OWASP Top-Ten)