

Kod szkolenia: J/SEC

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

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.

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 J/WEB1, J/WEB2).

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.

Parametry szkolenia:

2*7 godzin wykładów i warsztatów w proporcji 1/3.

Wielkość grupy: maks. 8-10 osób.

Polecane szkolenia poprzedzające:

J/JP, J/WEB2

Program szkolenia:

1. Wstęp

- Omówienie źródeł zagrożeń dla aplikacji Webowych (błędna konfiguracja, błędy w serwerach, błędy w aplikacji...)
- Omówienie różnych podejścia do bezpieczeństwa/paradygmaty (Defense in depth, security by obscurity, low hanging fruits)

2. Sesja w aplikacji Webowej

- Sposoby realizacji sesji w aplikacjach Webowych
- Obsługa sesji w najpopularniejszych technologiach
- Atak porwania sesji (ang. session hijacking) i sposoby zabezpieczenia się
- Dobre praktyki związane z obsługą sesji w aplikacjach Webowych
- Zapoznanie z programem WebScarab – narzędziem umożliwiającym testowanie bezpieczeństwa aplikacji

3. Ataki wstrzyknięcia (ang. injection attacks)

- Wprowadzenie do ataków wstrzyknięcia, powody ich występowania i metody zabezpieczenia (escapowanie oraz walidacja danych)
 - Realizacji walidacji w najpopularniejszych technologiach
 - Omówienie biblioteki AntiSamy, zapewniającej filtrowanie wpisywanych tagów HTML
 - Atak wstrzyknięcia na stronach bez pól tekstowych
 - SQL-Injection – nie tylko „or 1=1”
 - Nie tylko SQL-Injection (XML-Injection, X-PATH, Command Injection ...)
4. Atak CSRF (ang. Cross Site Request Forgery)
- Omówienie idei działania ataku typu CSRF, przykład
 - Metody zabezpieczenia się przed atakiem CSRF
5. Uwierzytelnienie i autoryzacja w aplikacjach Webowych
- Zapewnienie bezpiecznego sposobu uwierzytelniania
 - Polityka dotycząca haseł (czas życia, sposób przechowywania, itp. ...)
 - Realizacja uwierzytelniania w aplikacjach opartych na Java Enterprise Edition (JAAS) oraz znanych szkieletach (Seam, Spring)
6. Obsługa błędów w aplikacjach Webowych
- 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
- Problemy związane z wielowątkowością – wyścigi oraz nadpisanie danych
 - Cyklu życia dynamicznych stron i servletów na przykładach najpopularniejszych technologii
 - Omówienie przykładowego ataku wykorzystującego błędne zaimplementowanie wielowątkowości
8. Bezpieczeństwo WebServices
9. Niebezpieczeństwa języka Java
10. Bezpieczna konfiguracja serwerów aplikacyjnych
- Bezpieczna architektura dla aplikacji Webowych (wykorzystanie DMZ, filtrowanie adresów ...)

- Realizacja podmiany standardowej strony błędu
- 11. Inne zagadnienia związane z bezpieczeństwem
 - Zapewnienie poufności przesyłanych danych
 - 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
 - Logowanie błędów.
 - Zabezpieczenia w postaci niewidocznych linków
- 12. Jak pisać bezpieczne aplikacje
 - 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,...)
 - Gdzie znaleźć dodatkowe informacje o częstych, znanych błędach (CERT Secure-Coding, OWASP Top-Ten)