# Tytuł szkolenia: Bezpieczeństwo Aplikacji Webowych

## Kod szkolenia: W-BEZP-WEB2

## Wprowadzenie

Tworzysz lub zarządzasz aplikacją webową / stroną WWW? Chciałbyś odpowiednio ją zabezpieczyć? To szkolenie jest dla Ciebie! Dowiesz się z niego jak hakerzy przełamują zabezpieczenia aplikacji i do czego może to prowadzić. Dowiesz się też jak chronić swoją aplikację / stronę WWW oraz dane klientów przed atakami.

Na wstępie omówione zostaną podstawowe algorytmy kryptograficzne (kryptografia symetryczna, asymetryczna, podpisywanie, funkcje skrótu, certyfikaty) wraz z praktycznymi przykładami użycia.

Główna część szkolenia bazuje na liście OWASP Top 10 – dziesięciu najczęściej występujących błędów w aplikacjach webowych. Lista ta powstała w 2017 roku i opiera się na rzeczywistych danych uzyskanych od firm, organizacji i osób zawodowo zajmujących się testowaniem zabezpieczeń.

Każda kategoria z listy będzie dokładnie omówiona. W większości przypadków, podatności zostaną zaprezentowane w aplikacji napisanej specjalnie na potrzeby szkolenia. Na koniec każdej części aplikacja będzie poprawiana a omawiane błędy eliminowane. To wszystko w formie workshopu - uczestnicy dostaną obraz maszyny wirtualnej na którym będą mogli ćwiczyć poznane ataki i metody obrony. Interesujące będą zapewne przykłady z życia – omówienie konkretnych błędów w rzeczywistych aplikacjach.

Omówione zostaną następujące kategorie błędów:

- Błędy typu Injection
  Błędy SQL Injection, Command Injection i inne wstrzyknięcia.
- Niepoprawna obsługa uwierzytelniania i sesji
  Błędy umożliwiające ominięcie uwierzytelniania lub przejęcie sesji innego użytkownika.
- Ujawnienie poufnych danych
  Wszelkiego rodzaju błędy skutkujące ujawnieniem poufnych danych.
- XML External Entities (XXE)
  Błędy w parserach XML związane z obsługą encji zewnętrznych.
- Niepoprawna kontrola dostępu
  Błędy umożliwiające obejście kontroli dostępu – directory traversal, wgranie web-shell'a.
- Błędna konfiguracja zabezpieczeń
  Wszelkiego rodzaju błędy związane z niepoprawną konfiguracją środowiska i serwerów.
- Cross-Site Scripting (XSS)
  Błędy reflected XSS, persistent XSS, DOM based XSS.
- Niebezpieczna deserializacja
  Błędy związane z deserializacją obiektów umożliwiające zdalne wykonanie kodu.
- Używanie komponentów ze znanymi podatnościami
  Problemy związane z brakiem kontroli używanych komponentów.
- Niewystarczające logowanie i monitorowanie
  Problemy związane z niewystarczającym logowaniem i monitorowaniem poczynań użytkowników.
- Cross-Site Request Forgery (CSRF, XSRF)
  Błąd CSRF umożliwiający wykonanie pewnych akcji w ramach sesji zalogowanego użytkownika.
- Clickjacking
  Błąd umożliwiający przechwycenia kliknięcia i wykonanie niechcianej akcji.

## Adresaci szkolenia

Szkolenie kierowane jest do programistów i testerów chcących pogłębić swoją wiedzę na temat bezpieczeństwa aplikacji webowych. Aplikacja demonstracyjna napisana jest w Javie, ale większość ataków nie jest związana z jakimkolwiek językiem programowania czy technologią.

Aby w pełni skorzystać z tego szkolenia, uczestnicy powinni posiadać podstawową wiedzę z zakresu aplikacji webowych (podstawowe zasady działania), protokołu HTTP (podstawowa wiedza na temat budowy i cech żądań GET i POST), programowania (podstawy programowania w jakimkolwiek języku), Linuksa (ćwiczenia będą wykonywane w środowisku Kali Linux), SQL oraz Javascript.

## Cel szkolenia

Pozyskanie i usystematyzowanie wiedzy z dziedziny bezpieczeństwa aplikacji webowych. Poznanie najpopularniejszych ataków i metod ochrony.

## Czas i forma szkolenia

- 21 godzin (3 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

## Plan szkolenia

1. Wstęp do szkolenia
    a. Wprowadzenie
    b. Prezentacja środowiska
2. Podstawy kryptografii
    a. Kryptografia symetryczna
    b. Kryptograficzna funkcja skrótu (hash)
    c. Kryptografia asymetryczna
    d. Certyfikaty
3. Błędy typu Injection
    a. Wprowadzenie do SQL Injection
    b. Omijanie uwierzytelniania
    c. Wykradanie poufnych danych
    d. Metody ochrony
    e. Command Injection
4. Niepoprawna obsługa uwierzytelniania i sesji
    a. Najczęstsze błędy popełniane przy implementacji uwierzytelniania
    b. Zalecenia dotyczące implementacji uwierzytelniania
    c. Błędy popełniane przy implementacji obsługi sesji
    d. Atak Session Fixation
    e. Zalecenia dotyczące implementacji zarządzania sesjami
5. Ujawnienie poufnych danych
    a. Błędy i zapobieganie
6. XML External Entities (XXE)
    a. Wprowadzenie do XXE
    b. Atak XXE
    c. Ochrona przed XXE
7. Niepoprawna kontrola dostępu
    a. Wprowadzenie
    b. Directory Traversal
    c. Niezabezpieczone bezpośrednie referencje do obiektów
    d. Metody ochrony
    e. Błędy związane z implementacją wgrywania plików
    f. Metody ochrony
8. Błędna konfiguracja zabezpieczeń
    a. Wprowadzenie
    b. Przykłady
    c. Transport Layer Security
9. Cross-Site Scripting (XSS)
    a. Reflected XSS
    b. Persistent XSS
    c. DOM based XSS
    d. Ochrona przed XSS
    e. Content Security Policy (CSP)

10. Niebezpieczna deserializacja
    a. Wprowadzenie
    b. Atak na deserializację w Javie
    c. Metody ochrony
11. Używanie komponentów ze znanymi podatnościami
    a. Omówienie
    b. Przykłady
12. Niewystarczające logowanie i monitorowanie
13. Cross-Site Request Forgery (CSRF)
    a. Wprowadzenie
    b. Atak
    c. Metody ochrony
14. Clickjacking
    a. Wprowadzenie
    b. Atak
    c. Metody ochrony