Kod szkolenia: **PHP/SEC**

Tytuł szkolenia: **Bezpieczeństwo aplikacji internetowych w PHP**

Dni: 2

Opis:

Adresaci szkolenia:

Szkolenie przeznaczone jest dla programistów tworzących aplikacje internetowe w języku PHP, którzy chcą poznać najlepsze praktyki w kontekście bezpieczeństwa.

Cel szkolenia:

Bezpieczeństwo jest jednym z najważniejszych elementów, które należy wziąć pod uwagę podczas tworzenia aplikacji internetowych. Szkolenie ma na celu omówienie współczesnych problemów bezpieczeństwa aplikacji internetowych, zaprezentowania informacji na temat różnych metod dokonywania ataków oraz sposobów na zabezpieczenie się przed nimi.

Uczestnicy szkolenia w szczególności:
zdobędą wiedzę na temat różnych metod ataków na aplikacje internetowe,
przećwiczą sposoby obrony przed atakami podczas warsztatów,
dowiedzą się w jaki sposób konfigurować oraz przechowywać konfigurację aplikacji i serwera.

Wymagania:

Od uczestników wymagana jest podstawowa znajomość PHP 5 i SQL.

Parametry szkolenia:

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

Program szkolenia:

1. Wprowadzenie
    - Czym jest bezpieczeństwo?
    - Podstawowe pojęcia związane z tematem bezpieczeństwa
    - Kto i jak chce zaatakować Twoją aplikację?
    - Defense in Depth
    - Wytyczne co do tworzenia bezpiecznych aplikacji
    - Podsumowanie zagrożeń i przegląd OWASP Top 10
    - Katalogi podatności i exploitów

2. Rodzaje ataków i sposoby zabezpieczenia aplikacji
    - SQL Injection
    - Code Injection
        - Local File Inclusion
        - Remote File Inclusion
    - Command Injection
    - XSS Injection
    - XPath Injection
    - Log Injection
    - Path Traversal
    - Ataki XSRF / CSRF (Cross-site request forgery)
    - Clickjacking
    - Tabnabbing
    - Session Hijacking, Fixation, Adoption
3. Inne ważne elementy wpływające na bezpieczeństwo
    - Filtrowanie danych wejściowych
    - Wycieki informacji w aplikacjach
    - Dobre praktyki obsługi błędów
    - Szyfrowanie danych w PHP
    - Właściwe zarządzanie sesją użytkownika
    - Upload plików i autoryzowany dostęp do nich
    - Bezpieczeństwo i polityka haseł
    - Bezpieczna konfiguracja aplikacji i serwera
    - Bezpieczny AJAX po stronie serwera:
        - JSON/JavaScript Hijacking
        - Same-Origin Policy
        - JSON with Padding (JSONP)
        - Cross-Origin Resource Sharing (CORS)
        - Content-Security Policy (CSP)
4. Logowanie błędów i incydentów bezpieczeństwa
    - Systemy IDS, IPS, WAF
5. Podsumowanie, narzędzia, zasoby
    - Zasoby i narzędzia wspierające tworzenie bezpiecznych aplikacji internetowych w PHP