

SZKOLENIE ŚREDNIO ZAAWANSOWANE

Bezpieczeństwo aplikacji internetowych w PHP

PHP/SEC

Czas trwania: 2 dni (16h)

Cele szkolenia

- Omówienie współczesnych problemów bezpieczeństwa aplikacji internetowych
- Zaprezentowanie informacji na temat różnych metod dokonywania ataków oraz sposobów na zabezpieczenie się przed nimi
- Przećwiczenie sposobów obrony przed atakami podczas warsztatów
- Nauka konfiguracji oraz przechowywania konfiguracji aplikacji i serwera

Zalety

- Zdobyć wiedzy na temat różnych metod ataków na aplikacje internetowe
- Praktyka przed teorią - wszystkie szkolenia technologiczne prowadzone są w formie warsztatowej. Konieczna teoria jest wyjaśniana na przykładzie praktycznych zadań
- Konkretna umiejętność - w ramach każdego szkolenia rozwijamy praktyczne umiejętności związane z daną technologią i tematyką
- Nauka z praktykami - wszyscy trenerzy na co dzień pracują w projektach, gwarantuje to dostęp do eksperckiej wiedzy i praktycznego know-how

Dla kogo?

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

Wymagania

- Od uczestników wymagana jest podstawowa znajomość PHP 5 i SQL

Program

1. Wprowadzenie
 - a. Czym jest bezpieczeństwo?
 - b. Podstawowe pojęcia związane z tematem bezpieczeństwa
 - c. Kto i jak chce zaatakować Twoją aplikację?
 - d. Defense in Depth
 - e. Wytyczne co do tworzenia bezpiecznych aplikacji



- f. Podsumowanie zagrożeń i przegląd OWASP Top 10
- g. Katalogi podatności i exploitów
- 2. Rodzaje ataków i sposoby zabezpieczenia aplikacji
 - a. SQL Injection
 - b. Code Injection
 - Local File Inclusion
 - Remote File Inclusion
 - c. Command Injection
 - d. XSS Injection
 - e. XPath Injection
 - f. Log Injection
 - g. Path Traversal
 - h. Ataki XSRF/CSRF (Cross-site request forgery)
 - i. Clickjacking
 - j. Tabnabbing
 - k. Session Hijacking, Fixation, Adoption
- 3. Inne ważne elementy wpływające na bezpieczeństwo
 - a. Filtrowanie danych wejściowych
 - b. Wycieki informacji w aplikacjach
 - c. Dobre praktyki obsługi błędów
 - d. Szyfrowanie danych w PHP
 - e. Właściwe zarządzanie sesją użytkownika
 - f. Upload plików i autoryzowany dostęp do nich
 - g. Bezpieczeństwo i polityka haseł
 - h. Bezpieczna konfiguracja aplikacji i serwera
 - i. 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
 - a. Systemy IDS, IPS, WAF
- 5. Podsumowanie, narzędzia, zasoby
 - a. Zasoby i narzędzia wspierające tworzenie bezpiecznych aplikacji internetowych w PHP

