

kod szkolenia: BEZP_WEB / PL AA 2d

Bezpieczeństwo aplikacji webowych



Przeznaczenie szkolenia

Szkolenie przeznaczone jest dla praktyków IT – szczególnie deweloperów oraz testerów oprogramowania, ale również administratorów systemów i managerów, którzy chcą poznać obecnie stosowane formy ataków na aplikacje webowe oraz sposoby obrony przed nimi.



Korzyści wynikające z ukończenia szkolenia

Uczestnik szkolenia pozyska kompleksową, praktyczną, popartą licznymi przykładami oraz ćwiczeniami, wiedzę na temat najpopularniejszych form ataków na aplikacje webowe oraz sposobów obrony przed nimi.



Oczekiwane przygotowanie słuchaczy

- Podstawowa umiejętność programowania w dowolnym języku
- Podstawowa znajomość JavaScript oraz składni SQL
- Podstawowa znajomość architektury rozwiązań IT, aplikacji webowych, funkcjonowania systemów operacyjnych oraz sieci komputerowych



Język szkolenia

- Szkolenie: polski



Czas trwania

2 dni / 14 godzin

Agenda szkolenia

1. Wprowadzenie do bezpieczeństwa aplikacji webowych
 - Architektura aplikacji webowych
 - OWASP Top 10 2021
2. Bezpieczeństwo ruchu sieciowego
 - TLS/SSL
 - Nagłówki HTTP w kontekście bezpieczeństwa
 - Same-Origin Policy i Cross-Origin Resource Sharing (CORS)
3. Narzędzia
 - Analiza ruchu sieciowego
 - Manipulacja zapytaniami HTTP
 - Tworzenie własnych skryptów
 - Skanery podatności
4. Analiza podatności (atak, obrona, przykład)
 - Cross-site scripting (XSS)
 - Cross-Site Request Forgery (CSRF)
 - Directory Traversal
 - Unrestricted File Upload
 - Insecure Direct Object Reference (IDOR)
 - SQL i NoSQL injection
 - Server-Side Template Injection (SSTI)
 - Server-Side Request Forgery (SSRF)
 - Broken authentication and authorization
 - Denial of Service
5. Bezpieczeństwo API
 - Metody uwierzytelniania i autoryzacji
 - OWASP API Security Top 10 2019
6. Czarnoskrzynkowy test penetracyjny (CTF)