

Tytuł szkolenia: Cyberbezpieczeństwo dla webdeveloperów

Kod szkolenia: cyberbezpieczeństwo-dla-webdeveloperów

Wprowadzenie

Szkolenie z najważniejszych zagrożeń aplikacji webowych względem OWASP. Czas trwania to 7 godzin, w tym wykłady i warsztaty praktyczne.

Adresaci szkolenia

Szkolenie przeznaczone jest dla programistów aplikacji webowych w dowolnych technologiach od podstawowego doświadczenia.

Wymagania:

Od uczestników wymagana jest podstawowa wiedza na temat protokołu HTTP, ciastek i sesji.

Cel szkolenia

Celem szkolenia jest zwiększenie świadomości możliwych ataków na aplikacje webowe i wskazanie możliwych sposobów zabezpieczania tworzonych rozwiązań.

Czas i forma szkolenia

- 7 godzin (1 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

Plan szkolenia

1. Program szkolenia

- Najważniejsze wytyczne cyber - o OWASP, ich rekomendacjach i standardach
- Ogólne zasady cyber dla developerów - o błędach w kodzie, wdrożeniowych i analizie ryzyka
- Mity i fakty - najważniejsze informacje na temat sesji użytkowników, haseł i inne, powszechnie powielane błędy
- Największe ryzyka aplikacji webowych - przegląd zagrożeń i możliwe rozwiązania
- AI a cyberbezpieczeństwo - o bezpieczeństwie aplikacji tworzonych z pomocą AI i vibe codingu