



UKNOW EDU
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

Brak ocen dla tego dostawcy

Bezpieczeństwo aplikacji www

Numer usługi 2025/10/03/172284/3055035

2 800,00 PLN brutto

2 800,00 PLN netto

175,00 PLN brutto/h

175,00 PLN netto/h

📍 zdalna w czasie rzeczywistym

📄 Usługa szkoleniowa

🕒 16 h

📅 27.04.2026 do 28.04.2026

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

- programiści aplikacji internetowych,
- testerzy i specjaliści ds. QA,
- administratorzy systemów i sieci,
- specjaliści ds. cyberbezpieczeństwa,
- osoby odpowiedzialne za utrzymanie i rozwój aplikacji webowych,
- pracownicy działów IT zainteresowani podniesieniem kompetencji w zakresie bezpieczeństwa aplikacji www

Minimalna liczba uczestników

1

Maksymalna liczba uczestników

10

Data zakończenia rekrutacji

20-10-2025

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Liczba godzin usługi

16

Podstawa uzyskania wpisu do BUR

Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Uczestnik pozna główne zagrożenia dla aplikacji www oraz nauczy się identyfikować i zabezpieczać podatności (injection, XSS, CSRF, phishing). Nabędzie umiejętność stosowania dobrych praktyk w projektowaniu, testowaniu i utrzymaniu aplikacji internetowych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
1. Uczestnik zna podstawowe zagrożenia dla aplikacji www oraz mechanizmy ataków (injection, XSS, CSRF, phishing). 2. Uczestnik potrafi rozpoznać podatności w kodzie, stosować czyszczenie danych i wdrażać mechanizmy zabezpieczeń. 3. Uczestnik rozumie znaczenie bezpieczeństwa aplikacji w organizacji i potrafi stosować dobre praktyki w codziennej pracy.	Udzielenie co najmniej 70% poprawnych odpowiedzi w teście wiedzy.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1. Architektury aplikacji internetowych i źródła zagrożeń.
2. Ataki typu injection.
3. Ataki XSS.
4. Problemy z czyszczeniem danych.
5. Ograniczenia kodu w JavaScript.
6. Cross-site Request Forgery (CSRF).
7. Cache.
8. Socjotechnika i phishing.
9. Uwierzytelnianie.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 800,00 PLN
Koszt przypadający na 1 uczestnika netto	2 800,00 PLN
Koszt osobogodziny brutto	175,00 PLN
Koszt osobogodziny netto	175,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy szkolenia otrzymają materiały dydaktyczne w formie prezentacji multimedialnej, obejmującej wszystkie omawiane zagadnienia. Prezentacja zawiera treści teoretyczne oraz przykłady praktyczne związane z bezpieczeństwem aplikacji internetowych, atakami (injection, XSS, CSRF) i metodami ich zabezpieczania. Dzięki temu uczestnicy mogą w dowolnym momencie wrócić do omawianych treści i wykorzystać je w swojej pracy.

Warunki techniczne

Szkolenie realizowane online w czasie rzeczywistym za pośrednictwem platformy Zoom. Uczestnik musi dysponować komputerem z dostępem do internetu oraz kamerą i mikrofonem.

Kontakt



Alina Zhulmina

E-mail szkolenia@uknowedu.pl

Telefon (+48) 693 505 502