Możliwość dofinansowania

Comarch SA

★★★★½

Bezpieczeństwo aplikacji internetowych

Numer usługi 2025/04/28/7733/2714948

2 337,00 PLN brutto
1 900,00 PLN netto
146,06 PLN brutto/h
118,75 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
23.10.2025 do 24.10.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Identyfikator projektu	Małopolski Pociąg do kariery
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie przeznaczone jest dla programistów i projektantów tworzących aplikacje internetowe, którzy chcą nauczyć się jak budować aplikacje bezpieczne.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	16-10-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Szkolenie ma na celu zapoznanie uczestników z zagrożeniami aplikacji internetowych wynikającymi z ich szczególnej architektury. Po zakończeniu szkolenia jego uczestnik będzie potrafił zidentyfikować i zneutralizować potencjalne

problemy bezpieczeństwa aplikacji internetowych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Identyfikować zagrożenia bezpieczeństwa związane z aplikacjami internetowymi	Użytkownik wymienia i charakteryzuje podstawowe zagrożenia bezpieczeństwa, takie jak SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), ataki typu Man-in-the-Middle (MITM), czy nieautoryzowany dostęp. Użytkownik wskazuje źródła zagrożeń w aplikacjach webowych (np. nieprawidłowe walidacje danych wejściowych, brak odpowiednich nagłówków HTTP). Użytkownik rozumie konsekwencje potencjalnych zagrożeń dla aplikacji i użytkowników.	Test teoretyczny
Unikać błędów podczas tworzenia aplikacji internetowych powodujących luki bezpieczeństwa	Użytkownik stosuje techniki zabezpieczania aplikacji, takie jak prawidłowa walidacja i filtrowanie danych wejściowych, używanie parametrów w zapytaniach SQL, oraz unikanie hardkodowania haseł. Użytkownik rozumie zasady stosowania bezpiecznych praktyk kodowania, takich jak unikanie przestarzałych funkcji i zapewnianie ochrony przed atakami typu injection. Użytkownik wykazuje umiejętność stosowania bezpiecznych bibliotek i frameworków w kodowaniu aplikacji internetowych, unikając tych, które mają znane luki bezpieczeństwa. Użytkownik jest w stanie zidentyfikować i usunąć luki bezpieczeństwa, takie jak nadużywanie uprawnień, brak odpowiednich sesji i ciasteczek lub nieszyfrowane połączenia.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wytłumaczyć dlaczego bezpieczeństwo aplikacji jest ważne i dlaczego jest często bagatelizowane	Użytkownik wyjaśnia, jakie konsekwencje dla użytkowników i organizacji mogą wynikać z naruszenia bezpieczeństwa aplikacji (np. kradzież danych osobowych, straty finansowe, uszczerbek na reputacji). Użytkownik rozumie, dlaczego aplikacje webowe są szczególnie podatne na ataki i jakie wyzwania wiążą się z utrzymaniem ich bezpieczeństwa (np. szybko zmieniające się technologie, presja czasu, złożoność). Użytkownik umie uzasadnić, dlaczego w wielu przypadkach bezpieczeństwo jest ignorowane lub bagatelizowane, wskazując na brak wiedzy, zaniedbania lub priorytetowanie szybkości rozwoju	Test teoretyczny
Skonfigurować używane oprogramowanie pod względem bezpieczeństwa, rozumiejąc cel i zastosowanie występujących w nim zabezpieczeń	Użytkownik konfiguruje serwery i aplikacje webowe, uwzględniając zasady bezpieczeństwa, takie jak konfiguracja HTTPS, zabezpieczenie przed atakami typu DDoS, oraz zabezpieczenie serwera przed nieautoryzowanym dostępem. Użytkownik rozumie różnice między różnymi mechanizmami zabezpieczeń (np. SSL/TLS, zapory sieciowe, kontrola dostępu) i potrafi je prawidłowo zastosować do konkretnego oprogramowania. Użytkownik aktualizuje oprogramowanie, usuwając potencjalne luki bezpieczeństwa, oraz przeprowadza audyty bezpieczeństwa, aby ocenić stan zabezpieczeń systemu.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Skonfigurować bezpieczny system uwierzytelniania użytkowników z użyciem aktualnych praktyk projektowych i specyfikacji	Użytkownik konfiguruje system uwierzytelniania, wykorzystując nowoczesne techniki, takie jak OAuth2, OpenID Connect, lub JWT (JSON Web Tokens), zapewniając bezpieczny proces logowania. Użytkownik stosuje techniki ochrony haseł, takie jak haszowanie z użyciem algorytmów (np. bcrypt, PBKDF2), i unika przechowywania haseł w postaci tekstu jawnego. Użytkownik rozumie i stosuje wieloetapowe uwierzytelnianie (2FA) oraz umiejętnie konfiguruje odpowiednie mechanizmy w aplikacji. Użytkownik potrafi zabezpieczyć sesje użytkowników, stosując bezpieczne ciasteczka, zarządzanie sesjami oraz ochronę przed kradzieżą sesji.	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

Szczegółowy program szkolenia

Architektury aplikacji internetowych i źródła zagrożeń

- Od aplikacji UTC do RIA
- Podstawowe problemy bezpieczeństwa: sesje, cookies, tokeny
- Problemy bezpieczeństwa w aplikacjach responsywnych
- Klasyfikacje zagrożeń: STRIDE, OWASP
- Najprostsze ataki fałszujące request

Ataki typu injection

- SQL Injection
- Blind Injection
- Code Injection
- Command Injection

Ataki XSS

- Scenariusz ataku – reflected XSS, persistent XSS
- Możliwości i ograniczenia Javascript, Source & Sink
- DOM-based XSS
- Problemy z czyszczeniem danych
- Etapy czyszczenia danych i ich ograniczenia

Ograniczenia kodu w Javascript

- Same Origin Policy
- CORS – działanie i konfiguracja
- Preflight

Cross-site Request Forgery (CSRF)

- Zasada działania
- Możliwości
- Sposoby zabezpieczenia

Nagłówki request i response dotyczące zabezpieczeń

Cache

- Zabezpieczenie przed click-jacking
- Specjalne nagłówki serwerów i przeglądarek
- Content Security Policy

Socjotechnika i phishing

- Człowiek jako podstawowe słabe ogniwo
- Możliwości preparowania linków

Uwierzytelnianie

- Klasyczne ataki na sesje I zabezpieczenia przed nimi
- Zabezpieczanie za pomocą JWT – zalety i wady
- OAuth 2
- OpenID Connect

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	2 337,00 PLN
Koszt przypadający na 1 uczestnika netto	1 900,00 PLN
Koszt osobogodziny brutto	146,06 PLN
Koszt osobogodziny netto	118,75 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Paweł Kasprowski

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik otrzymuje zestaw materiałów szkoleniowych w postaci podręczników rekomendowanych do realizacji szkolenia oraz ćwiczeń.

W czasie zajęć wykorzystywane są autorskie materiały dydaktyczne przygotowane przez wykładowcę oraz inne materiały dydaktyczne przygotowane przez organizatora szkolenia.

Warunki uczestnictwa

Warunkiem skorzystania ze szkolenia jest dokonanie równolegle rejestracji na kurs na stronie www.comarch.pl/szkolenia w formie:

- elektronicznego zamówienia szkolenia (przycisk "Zamów" przy wybranym temacie i terminie). Opcja ta dotyczy osób fizycznych oraz firm/instytucji

albo

- poprzez uzupełnienie i odesłanie na adres szkolenia@comarch.pl tradycyjnego formularza zgłoszeniowego który jest dostępny na stronie www.comarch.pl/szkolenia (przycisk "Pobierz formularz zgłoszeniowy"). Opcja ta dotyczy wyłącznie firm/Instytucji.

W obu przypadkach przy dokonaniu zgłoszenia prosimy o informacje dotyczącą projektu z którego dofinansowania korzysta Uczestnik.

Planowana przerwa: –obiadowa 60 min plus 2 kawowe po 15 minut.

Przerwa obiadowa w godzinach: 13:00

Przerwy kawowe: 11:00 i 15:00

Wykładowca ma prawo zmienić godziny przerw, jeśli wymaga tego proces dydaktyczny (np. rozpoczęte ćwiczenie) lub na życzenie większości uczestników kursu (zmęczenie, większa trudność treści kształcenia).

Informacje dodatkowe

Szkolenie Zdalne prowadzone jest w czasie rzeczywistymi i transmitowane za pomocą kanału internetowego z wykorzystaniem systemu ZOOM lub Webex, który umożliwia komunikację głosową oraz wideo z Uczestnikami przebywających w dowolnym miejscu ze sprawnie działającym stałym łączem internetowym. Każdy z uczestników szkolenia otrzymuje przed szkoleniem link dostarczony w wiadomości mailowej z informacjami dotyczącymi szkolenia zdalnego. Link umożliwiający uczestnictwo w spotkaniu jest ważny do momentu zakończenia szkolenia.

Szkolenie zakończone jest testem wiedzy z zakresu tematycznego omawianego na szkoleniu.

Szkolenie może być nagrywane /rejestrowane w celu kontroli/audytu zgodnie z Regulaminem Świadczenia Usług Szkoleniowych Organizatora.

Uczestnicy szkolenia otrzymają materiały szkoleniowe w wersji elektronicznej.

Warunki techniczne

Wymagania techniczne:

- Komputer / laptop ze stałym dostępem do Internetu (Szybkość pobierania/przesyłania: minimalna 2 Mb/s / 128 kb/s; zalecana 4 Mb/s / 512 kb/s
- przeglądarka internetowa – zalecane: Google Chrome, Mozilla Firefox, Microsoft Edge
- słuchawki lub dobrej jakości głośniki
- mikrofon

Zalecane

- dodatkowy monitor
- kamera (w przypadku komputerów stacjonarnych)
- spokojne miejsce, odizolowane od zewnętrznych czynników rozpraszających
- podstawowa znajomość języka angielskiego (do sprawnego poruszania się po platformie zdalnej)

Kontakt

Aneta Lewkowska

E-mail szkolenia@comarch.pl

Telefon (+48) 12 6877 811