Możliwość dofinansowania

Bezpieczeństwo aplikacji internetowych. Podstawy zabezpieczania aplikacji internetowych.

Numer usługi 2026/03/17/7733/3411323

2 337,00 PLN brutto
1 900,00 PLN netto
146,06 PLN brutto/h
118,75 PLN netto/h
183,33 PLN cena rynkowa

Comarch SA

4,5 / 5

1 063 oceny

Usługa szkoleniowa
zdalna w czasie rzeczywistym
16:00 h
20.07.2026 do 21.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Aplikacje biznesowe
Identyfikatory projektów	Kierunek - Rozwój, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe, Regionalny Fundusz Szkoleniowy II
Grupa docelowa usługi	**Profil uczestników** Szkolenie przeznaczone jest dla osób znających podstawy działania aplikacji internetowych chcących się dowiedzieć jakie zagrożenia bezpieczeństwa występują w tego typu aplikacjach i jak się przed nimi zabezpieczać. **Przygotowanie uczestników** • Od uczestników szkolenia wymagana jest znajomość zasad programowania oraz sposobu działania sieci WWW. Przydatna jest też choćby podstawowa znajomość języka Java. **Czas trwania kursu wynosi 16 godzin lekcyjnych, godzina lekcyjna to 45 minut.** **Usługa jest dedykowana dla uczestników projektu Małopolski pociąg do kariery.** *Usługa również adresowana dla uczestników projektu Małopolskie Bony rozwojowe Plus" i "Małopolski Pociąg do Kariery"* "Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	14-07-2026

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	wskazuje przykłady typowych podatności w aplikacjach internetowych, analizuje scenariusze ataków na aplikacje webowe, ocenia wpływ zidentyfikowanych zagrożeń na bezpieczeństwo systemu.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje zasady bezpiecznego tworzenia aplikacji internetowych.	identyfikuje błędy projektowe prowadzące do powstawania luk bezpieczeństwa, stosuje dobre praktyki programistyczne zwiększające bezpieczeństwo aplikacji, analizuje kod aplikacji pod kątem potencjalnych podatności.	Test teoretyczny z wynikiem generowanym automatycznie
Uzasadnia znaczenie bezpieczeństwa aplikacji internetowych w procesie wytwarzania oprogramowania.	wskazuje konsekwencje braku odpowiednich zabezpieczeń aplikacji, opisuje czynniki wpływające na pomijanie zagadnień bezpieczeństwa w projektach IT, analizuje przykłady incydentów bezpieczeństwa związanych z aplikacjami internetowymi.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Konfiguruje oprogramowanie z uwzględnieniem wymagań bezpieczeństwa.	identyfikuje dostępne mechanizmy zabezpieczeń w wykorzystywanym oprogramowaniu, konfiguruje ustawienia bezpieczeństwa zgodnie z zalecanymi praktykami, weryfikuje poprawność zastosowanych konfiguracji.	Test teoretyczny z wynikiem generowanym automatycznie
Konfiguruje bezpieczny mechanizm uwierzytelniania użytkowników w aplikacji internetowej.	dobiera mechanizmy uwierzytelniania zgodne z aktualnymi praktykami projektowymi, konfiguruje proces logowania użytkowników w aplikacji, stosuje mechanizmy ochrony danych uwierzytelniających, weryfikuje poprawność działania wdrożonego mechanizmu uwierzytelniania.	Test teoretyczny z wynikiem generowanym automatycznie

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.Usługa jest realizowana w godzinach lekcyjnych, tj. za godzinę usługi szkoleniowej rozumie się 45 minut, łącznie 16 godzin lekcyjnych.

Planowane przerwy w trakcie zajęć: 10:30-10:45, 13:00-13:30, 14:45-15:00. Przerwy nie są wliczone w godziny zajęć usługi. Liczba godzin zajęć praktycznych: 8 godzin lekcyjnych , liczba godzin zajęć teoretycznych: 8 godzin lekcyjnych, w tym test 10 min.

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).

2.Grupa docelowa: szkolenie przeznaczone jest dla osób znających podstawy działania aplikacji internetowych chcących się dowiedzieć jakie zagrożenia bezpieczeństwa występują w tego typu aplikacjach i jak się przed nimi zabezpieczać.

Przygotowanie uczestników: od uczestników szkolenia wymagana jest znajomość zasad programowania oraz sposobu działania sieci WWW. Przydatna jest też choćby podstawowa znajomość języka Java.

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 pozycji harmonogramu: 0

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

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

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

Radosław Janiak

trener Python, Java, SpringBoot, Hibernate, SQL, Docker, C++, C, Git, Thymleaf, powershell, bash, Windows, Linux; współpraca z Centrum Szkoleniowym od 2022; nauczyciel programowania dla dzieci i dorosłych oraz trener bootcampu; praktykujący programista

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Podręczniki w formie elektronicznej

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 30 min plus 2 kawowe po 15 minut.

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 zakończone jest testem wiedzy z zakresu tematycznego omawianego na szkoleniu.

Szkolenie może być zwolnione z VAT-u w zależności od rodzaju dofinasowania

Zawarto umowę z WUP Kraków na rozliczanie Usług z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu „Małopolski Pociąg do Kariery” i "Małopolskie Bony Rozwojowe Plus"

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

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój.

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)

Informacje dodatkowe

Szkolenie Zdalne prowadzone jest w czasie rzeczywistymi i transmitowane za pomocą kanału internetowego z wykorzystaniem systemu ZOOM, 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.

Kontakt

Aneta Lewkowska

E-mail aneta.lewkowska@comarch.pl
Telefon (+48) 12 6877 811