



Fundacja CODE:ME



Web Security. Bezpieczeństwo aplikacji webowych - kurs zdalny

Numer usługi 2024/09/23/32642/2323169

📍 zdalna w czasie rzeczywistym

📄 Usługa szkoleniowa

🕒 12 h

📅 14.10.2024 do 23.10.2024

920,00 PLN brutto

920,00 PLN netto

76,67 PLN brutto/h

76,67 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	<p>Kurs przeznaczony jest dla wszystkich osób posiadających podstawową wiedzę w zakresie aplikacji WWW (podstawy HTML, JS, CSS), które są zainteresowane aby poszerzyć swoją wiedzę o aspekty związane z bezpieczeństwem.</p> <p>Kurs dedykujemy zwłaszcza osobom rozważającym rozpoczęcie swojej kariery w kierunku Cyberbezpieczeństwo a także wszystkim, którzy zafascynowani są Cybersecurity.</p>
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	11-10-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	12
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Kurs przygotowuje do zdobycia umiejętności pozwalających uczestnikowi lepiej chronić swoje aplikacje internetowe przed atakami i zwiększyć bezpieczeństwo swoich systemów i użytkowników.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik: - identyfikuje i naprawia najczęściej spotykane błędy i podatności aplikacji WWW, - identyfikuje metody testowania bezpieczeństwa aplikacji WWW - identyfikuje techniki łatania podatności w aplikacjach WWW.	- rozróżnia najczęstsze luki bezpieczeństwa z listy OWASP Top 10 - definiuje różnice między http a https - analizuje nagłówki i ich role w zabezpieczeniu aplikacji - definiuje rekonesans aplikacji - definiuje koncepcję Shift-Left	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, dokument zawiera efekty uczenia się, do których uzyskania uczestnik przygotowywał się w procesie uczenia się.

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

Tak, dokument potwierdza, że walidacja została przeprowadzona zgodnie z ustalonymi kryteriami weryfikacji zawartymi w efektach uczenia się.

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

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Spotkanie nr 1:

1. Wstęp
2. Shift-Left czyli o Secure Software Development Lifecycle
3. OWASP Top 10
4. OWASP ASVS i inne standardy
5. Rekonesans
6. Jak działa przeglądarka?
7. HTTPS - Czym się różni http od https?
8. Nagłówki HTTP

Spotkanie nr 2:

1. Broken Access Control
2. Client-Side Request Forgery
3. Server-Side Request Forgery
4. Cryptographic Failures/Sensitive Data Exposure
5. Security misconfiguration i XXE (External XML Entities)

Spotkanie nr 3 :

1. Injections - XSS, SQLi, No-SQL injection, Command injection

Spotkanie nr 4 :

1. Identification and Authentication Failures
2. Software and Data Integrity Failures
3. Security Logging and Monitoring Failures
4. Vulnerability Management
5. Hardening infrastruktury

Harmonogram

Liczba przedmiotów/zajęć: 5

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 5 Web Security. Bezpieczeństwo aplikacji webowych - zajęcia 1	Wiktor Kierzek	14-10-2024	17:00	20:00	03:00
2 z 5 Web Security. Bezpieczeństwo aplikacji webowych - zajęcia 2	Wiktor Kierzek	16-10-2024	17:00	20:00	03:00
3 z 5 Web Security. Bezpieczeństwo aplikacji webowych - zajęcia 3	Wiktor Kierzek	21-10-2024	17:00	20:00	03:00
4 z 5 Web Security. Bezpieczeństwo aplikacji webowych - zajęcia 4	Wiktor Kierzek	23-10-2024	17:00	19:30	02:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 5 Web Security. Bezpieczeństwo aplikacji webowych - walidacja (weryfikacja wiedzy)	-	23-10-2024	19:30	20:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	920,00 PLN
Koszt przypadający na 1 uczestnika netto	920,00 PLN
Koszt osobogodziny brutto	76,67 PLN
Koszt osobogodziny netto	76,67 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Wiktor Kierzek

Ekspert w dziedzinie Cyberbezpieczeństwa
Specjalista do spraw cybersecurity z ponad 10 letnim doświadczeniem w branży. Aktualnie pełni rolę Senior IT Security Engineer w spółce Żabka Polska, a poza pracą prowadzi liczne szkolenia z cyber awareness. Można go spotkać na konferencjach branżowych, gdzie chętnie występuje w roli prelegenta. Swoją karierę w świecie IT rozpoczął jako programista a na swoim koncie może pochwalić się współpracą z m.in. Politechniką Poznańską - swoją Alma Mater, Cognifide, Codility czy Microsoftem. Jego umiejętności poświadczają liczne certyfikaty z zakresu cybersecurity takie jak CISSP, CCSKv4, CCSP, OSWE oraz OSCP. Jako główne zainteresowania zawodowe Wiktor wymienia bezpieczeństwo chmur, aplikacji internetowych i mobilnych, przetwarzanie rozproszone.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik przed rozpoczęciem szkolenia otrzyma informacje organizacyjne jak przygotować się do szkolenia. W trakcie kursu uczestnik otrzyma materiały szkoleniowe w postaci prezentacji (pliki pdf).

Warunki uczestnictwa

Aby móc aktywnie i efektywnie wziąć udział w szkoleniu wymagana jest znajomość podstaw HTML, JavaScript i CSS. Pomocne będą również podstawy SQL i znajomość conajmniej jednego, wybranego języka Backendowego (np. Java, Python) albo opcjonalnie umiejętność czytania i analizowania kodu.

Warunki techniczne

- rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa - **zoom**
- minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji - **laptop/komputer z dostępem do internetu oraz mikrofonem i kamerką**. Zalecamy korzystanie z dwóch monitorów podczas kursu.
- minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik - **stałe połączenie WI-FI/ Internet, minimalna przepustowość 10mb/s**
- okres ważności linku umożliwiającego uczestnictwo w spotkaniu on-line - **link dostępny jedynie w czasie trwania zajęć (czas rzeczywisty)**

Kontakt



Paulina Radwańska-Zubrzycka

E-mail kontakt@codeme.pl

Telefon (+48) 537 492 774