Możliwość dofinansowania

Szkolenie z Cyberbezpieczeństwa: Szkolenie z Bezpieczeństwa Webaplikacji (atakowanie i ochrona aplikacji webowych)

Numer usługi 2026/02/04/148153/3306956

6 750,24 PLN brutto
5 488,00 PLN netto
482,16 PLN brutto/h
392,00 PLN netto/h
196,00 PLN cena rynkowa

Niebezpiecznik.pl
Piotr Konieczny

4,7 / 5
30 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
14 h
16.07.2026 do 17.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie kierujemy przede wszystkim do osób, których praca ociera się o aplikacje webowe, a więc: • programistów i testerów, • administratorów oraz architektów i projektantów systemów komputerowych • audytorów i pentesterów, ...ale tak naprawdę, z otwartymi rękami powitamy każdą osobę która chce podnosić swoje kwalifikacje i wiedzę w temacie bezpieczeństwa aplikacji internetowych — dla nas wszyscy jesteście żądnymi wiedzy ludźmi, a nie stanowiskami ;-)
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	16
Data zakończenia rekrutacji	08-07-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	14
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Głównym celem szkolenia jest dostarczenie oraz poprawienie kompetencji uczestnika z zakresu Bezpieczeństwa Webaplikacji. Po zakończonym szkoleniu uczestnik podniesie poziom bezpieczeństwa w swojej firmie oraz rozwiąże najczęściej pojawiające się problemy, samodzielnie realizując metody rozwiązania na poziomie zaawansowanym, z maksymalnym wykorzystaniem swoich nowo nabytych umiejętności.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Po zakończonym szkoleniu uczestnik podniesie poziom bezpieczeństwa w swojej firmie oraz rozwiąże najczęściej pojawiające się problemy, samodzielnie realizując metody rozwiązania na poziomie zaawansowanym, z maksymalnym wykorzystaniem swoich nowo nabytych umiejętności.	Laboratoria przygotowane na symulowanym środowisku kształcenia.	Obserwacja w warunkach symulowanych

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

Z dokładnymi terminami tego szkolenia zapoznać się można pod poniższym linkiem:

https://niebezpiecznik.pl/szkolenia/atakowanie-ochrona-www/?zai

Po wybraniu terminu prosimy o kontakt mailowy: szkolenia@niebezpiecznik.pl

Współczesne problemy bezpieczeństwa aplikacji webowych

- zagrożenia wynikające z architektury webaplikacji (np. CGI, SSI, etc.)
- zagrożenia wynikające z języków programowania (PHP, JS, etc.) i technologi, np. ASP, JSP
- problem styku webaplikacji z bazą danych
- interfejsy zewnętrzne webaplikacji
- zagrożenia po stronie serwera, środowiska, sieci, a zagrożenia po stronie klienta
- zagrożenia stron tworzonych pod urządzenia mobilne (telefony, tablety)

Ataki na aplikacje webowe

- Wyszukiwanie adresów serwerów deweloperskich
- Bezpieczeństwo hostingu i webserwera
- Brak obsługi błędów
- Manipulacje parametrami (metody GET, POST)
- Techniki podsłuchu i manipulowania transmisją
- Atak Forcefull browsing
- Atak Path Traversal
- Technika Google Hacking
- Wstrzyknięcie kodu (PHP shell) i komend systemowych do webaplikacji
- Problem filtrowania danych wejściowych
- Ataki XSS (persistent, reflected)
- Omijanie filtrowania danych wejściowych i encodingu wyjściowych
- Ataki na sesję aplikacji webowej
- Podsłuchiwanie sesji i kradzież ciasteczek HTTP
- Jak poprawnie zarządzać sesją w webapikacji?
- Ataki CSRF/XSRF
- Bezpieczny upload plików
- Metody ułatwiające przetrwanie ataków DoS/DDoS
- Ataki Clickjacking
- Ataki na bazy danych
- Ataki SQL injection i Blind SQL injection
- Ochrona przed atakami SQL injection
- Szyfrowanie połączenia i ataki na SSL
- Szyfrowanie danych w webaplikacji
- Ochrona przed spamem i enumeracją zasobów oraz haseł
- Podsumowanie zagrożeń i przegląd OWASP TOP10
- Pozaprogramistyczne środki ochrony (systemy IDS/IPS, WAF)
- Omijanie detekcji przez systemy WAF/IDS/IPS

Problemy przeglądarek

- Same Orgin Policy
- Rich Internet Applications
- Dziury w przeglądarkach
- Ataki DNS-Rebinding
- Narzędzia podnoszące bezpieczeństwo i pomagające w testowaniu aplikacji webowych

Przegląd narzędzi automatyzujących wykrywanie podatności

Harmonogram

Liczba przedmiotów/zajęć: 4

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 4 Współczesne problemy bezpieczeństwa aplikacji webowych	Tomasz Borek	16-07-2026	10:00	13:00	03:00
2 z 4 Ataki na aplikacje webowe	Tomasz Borek	16-07-2026	13:00	17:00	04:00
3 z 4 Problemy przeglądarek	Tomasz Borek	17-07-2026	10:00	14:00	04:00
4 z 4 Przegląd narzędzi automatyzujących wykrywanie podatności	Tomasz Borek	17-07-2026	14:00	17:00	03:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 750,24 PLN
Koszt przypadający na 1 uczestnika netto	5 488,00 PLN
Koszt osobogodziny brutto	482,16 PLN
Koszt osobogodziny netto	392,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Tomasz Borek

W ramach firmy Niebezpiecznik.pl szkolę z zakresu Programowania Defensywnego (mój własny autorski program, z którym przyszedłem do Niebezpiecznika), Ataków i Ochrony Aplikacji Sieciowych oraz Bezpieczeństwa w Testach dla QA.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

1. Materiały szkoleniowe (zapis prezentacji).

Warunki uczestnictwa

Każdy uczestnik naszych szkoleń **musi** podpisać deklarację, że poznane ataki i narzędzia będzie wykorzystywał wyłącznie w celu testowania bezpieczeństwa swoich własnych sieci i webaplikacji.

Szkolenie odbywa się w formule BYOL (Bring Your Own Laptop). Wymagania: 2GB RAM, 5GB HDD oraz zainstalowany darmowy i dostępny na każdy system operacyjny program VirtualBox — trener przed startem szkolenia udostępni obraz maszyny wirtualnej na której będą odbywały się laboratoria.

Informacje dodatkowe

Z dokładnymi terminami tego szkolenia zapoznać się można pod poniższym linkiem:

https://niebezpiecznik.pl/szkolenia/atakowanie-ochrona-www/?zai

Po wybraniu terminu prosimy o kontakt mailowy: szkolenia@niebezpiecznik.pl

Warunki techniczne

Proszę upewnić się, aby na szkolenie zabrać własny laptop, posiadający minimum 3 GB RAM (rekomendowane 4+ GB) i co najmniej 10 GB wolnej przestrzeni na dysku. Konieczne będą też uprawnienia administratorskie pozwalające na wyłączenie wszelkiego rodzaju oprogramowania antywirusowego i rekonfigurację firewalla.

Kontakt

Magda Kowalska

E-mail szkolenia@niebezpiecznik.pl
Telefon (+48) 124 420 244