Możliwość dofinansowania

Szkolenie z Cyberbezpieczeństwa: Szkolenie z Bezpieczeństwa w Testach Oprogramowania (szkolenie dla QA)

Numer usługi 2026/08/11/148153/3741243

6 504,24 PLN brutto
5 288,00 PLN netto
464,59 PLN brutto/h
377,71 PLN netto/h
261,33 PLN cena rynkowa

Niebezpiecznik.pl
Piotr Konieczny

4,7 / 5

30 ocen

Kraków
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
14:00 h
30.12.2026 do 31.12.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie kierujemy przede wszystkim do osób, których praca związana jest z zapewnieniem jakości oraz testowaniem oprogramowania, a więc: • Testerów (manualnych oraz automatyzujących) i Inżynierów ds. zapewniania jakości • Audytorów i pentesterów ...ale tak naprawdę, z otwartymi rękami powitamy każdą osobę która chce podnosić swoje kwalifikacje i wiedzę w temacie testów bezpieczeństwa – dla nas wszyscy jesteście żądnymi wiedzy ludźmi, a nie stanowiskami ;-)
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	22-12-2026
Forma prowadzenia usługi	stacjonarna
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 w Testach Oprogramowania. 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 lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają 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/bezpieczenstwo-w-testach-oprogramowania-dla-qa/?zai

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

Tematyka szkolenia, wybrane zagadnienia:

- **Narzędzia deweloperskie przeglądarki oraz narzędzia typu lokalnego Proxy i ich wykorzystanie podczas testów bezpieczeństwa**Narzędzia deweloperskie przeglądarki w kontekście testów bezpieczeństwa
  - Instalacja i konfiguracja Burp Suite i OWASP ZAP
  - Przechwytywanie i modyfikacja żądań
  - Podmiana nagłówków żądania pozwalająca np. na podszywanie się pod Googlebot lub na omijanie WAF
  - **Omówienie zakresu podstawowych testów bezpieczeństwa aplikacji webowych i web serwisów, najczęstszych podatności i sposobów ich wykrywania (z wykorzystaniem Burp Suite)**Testy pod kątem najczęściej występujących podatności aplikacji webowych m. in. SQL Injection, XSS, CSRF
  - Testy walidacji po stronie serwera poprzez próbę ominięcia walidacji zapewnianej przez GUI
  - Testy dostępu do danych i plików bez zalogowania lub przez użytkowników z innym zakresem uprawnień
  - Testy poprawnego zarządzania sesją użytkownika
  - Testy wymagające dobrej znajomości logiki biznesowej aplikacji
  - Zagrożenia związane z przekazywaniem loginów/haseł/danych osobowych w URL i ich cachowaniem
  - Jakie dane nie powinny być zapisywane w logach?
  - Testy pod kątem najczęściej występujących podatności web serwisów m. in. XXE, Billion Laughs, CDATA Injection
  - proxy narzędzia do testów bezpieczeństwa
  - Najczęstsze błędy konfiguracyjne np. braki nagłówków, ich nieprawidłowa konfiguracja, stacktrace, słabe algorytmy SSL/TLS
  - Omówienie motywacji stojącej za wykonywaniem takich testów na wczesnych etapach projektu
  - Jak rozszerzyć testy funkcjonalne aby znajdować błędy bezpieczeństwa?
  - **Bezpieczeństwo i użyteczność**Jak powinny wyglądać czytelne komunikaty w zakresie bezpieczeństwa i prywatności użytkownika?
  - Użyteczność haseł i jak przekonać użytkownika do korzystania z bezpiecznego hasła?
  - Jak ograniczać czasu trwania sesji i dozwoloną liczbę sesji? Przykładowe rozwiązania z serwisów społecznościowych i stron banków.
  - Case study na przykładzie konfiguracji ustawień prywatności użytkownika
  - Case study na przykładzie komunikatów przeglądarek informujących o ostrzeżeniach dotyczących certyfikatów SSL/TLS
  - Dlaczego trzeba zwrócić uwagę na Privacy by Design i Privacy by Default?
  - **Testy wydajnościowe z użyciem narzędzia JMeter w kontekście bezpieczeństwa**Testy obciążeniowe, przeciążeniowe i ataki DoS
  - Rodzaje ataków DoS
  - JMeter i proxy narzędzia do testów bezpieczeństwa
  - Symulacja ataków z różnych adresów IP poprzez IP Spoofing
  - Wykorzystanie skryptów JMetera do automatycznego skanowania bezpieczeństwa
  - Automatyczne testy bezpieczeństwa z wykorzystaniem JMtera
  - Inne narzędzia do testów DoS
  - Fuzzing z wykorzystaniem JMetera
  - **Automatyzacja testów bezpieczeństwa (z wykorzystaniem OWASP ZAP, Selenium Webdriver i Pythona)**Przegląd najpopularniejszych skanerów, zarówno płatnych jak i open source
  - Omówienie skanerów Burp Suite Professional oraz OWASP ZAP
  - Omówienie często występujących błędów łatwych do wykrycia za pomocą testów automatycznych
  - Automatyczne testy bezpieczeństwa jako element procesów CI/CD
  - Omówienie możliwości OWASP ZAP API i konfiguracja automatycznego skanowania
  - Wykorzystanie testów automatycznych w Selenium do przeprowadzenia testów bezpieczeństwa
  - Automatyczne zgłaszanie błędów lub aktualizacja ich statusu z wykorzystaniem JIRA REST API
  - Automatyczne generowanie raportu z testów
  - Weryfikacja raportów z testów pod kątem wyników fałszywie pozytywnych
  - **Testy bezpieczeństwa jako element testów akceptacyjnych**Jak przygotować plany i scenariusze testów bezpieczeństwa i na jakie dokumenty i metodyki warto się powoływać?
  - Przykładowe dokumenty OPZ i SIWZ zawierające wymagania na testy
  - bezpieczeństwa/penetracyjne
  - Przykładowe wymagania pozafunkcjonalne w zakresie bezpieczeństwa do uwzględnienia w dokumentacji testowej
  - Praktyczne przykłady pokrycia wymagań bezpieczeństwa w przypadkach testowych
  - Jak dzięki niewielkim modyfikacjom można dostosować istniejący przypadek testowy, aby zapewniał pokrycie testami bezpieczeństwa?
  - Wskazówki dotyczące przygotowania raportu z testów bezpieczeństwa
  - Przykłady wymaganych kompetencji m. in. w zakresie certyfikacji
  - **Od testera do pentestera**Jak pokierować karierą aby zdobyć większe doświadczenie w zakresie testów bezpieczeństwa?
  - Wskazówki dotyczące dalszej nauki, dokumenty, książki i metodyki, które warto poznać oraz certyfikacja w zakresie bezpieczeństwa
  - **Omówienie dokumentów:**OWASP Testing Guides
  - OWASP ASVS
  - OWASP TOP10
  - **Podstawowe certyfikaty z zakresu testów bezpieczeństwa:**CEH
  - CompTIA Security+
  - ISTQB Security Tester

Każdy z podpunktów związany jest z praktycznym ćwiczeniem. Podczas omawiania konkretnego ataku albo podatności lub narzędzia, które je wykorzystują, zawsze pokazujemy jak zabezpieczyć aplikację przed tym problemem. Dla przejrzystości konspektu, nie zostało to wyszczególnione powyżej.

Harmonogram

Liczba pozycji harmonogramu: 12

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 12 Narzędzia deweloperskie przeglądarki oraz narzędzia typu lokalnego Proxy i ich wykorzystanie podczas testów bezpieczeństwa	Zajęcia	Tomasz Borek	30-12-2026	10:00	12:00	02:00
2 z 12 Omówienie zakresu podstawowych testów bezpieczeństwa aplikacji webowych i web serwisów, najczęstszych podatności i sposobów ich wykrywania (z wykorzystaniem Burp Suite)	Zajęcia	Tomasz Borek	30-12-2026	12:00	13:00	01:00
3 z 12 -	Przerwa	-	30-12-2026	13:00	14:00	01:00
4 z 12 Bezpieczeństwo i użyteczność	Zajęcia	Tomasz Borek	30-12-2026	14:00	16:00	02:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 12 Testy wydajnościowe z użyciem narzędzia JMeter w kontekście bezpieczeństwa	Zajęcia	Tomasz Borek	30-12-2026	16:00	17:00	01:00
6 z 12 Automatyzacja testów bezpieczeństwa (z wykorzystaniem OWASP ZAP, Selenium Webdriver i Pythona)	Zajęcia	Tomasz Borek	31-12-2026	10:00	11:00	01:00
7 z 12 Testy bezpieczeństwa jako element testów akceptacyjnych	Zajęcia	Tomasz Borek	31-12-2026	11:00	12:00	01:00
8 z 12 Od testera do pentestera	Zajęcia	Tomasz Borek	31-12-2026	12:00	13:00	01:00
9 z 12 -	Przerwa	-	31-12-2026	13:00	14:00	01:00
10 z 12 Omówienie dokumentów	Zajęcia	Tomasz Borek	31-12-2026	14:00	15:00	01:00
11 z 12 Podstawowe certyfikaty z zakresu testów bezpieczeństwa	Zajęcia	Tomasz Borek	31-12-2026	15:00	16:00	01:00
12 z 12 -	Walidacja	-	31-12-2026	16:00	17:00	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	14:00
w tym suma godzin zajęć	11:00
w tym suma godzin walidacji	01:00
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	16:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 504,24 PLN
Koszt przypadający na 1 uczestnika netto	5 288,00 PLN
Koszt osobogodziny brutto	464,59 PLN
Koszt osobogodziny netto	377,71 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	14:00

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

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 aplikacji własnych lub aplikacji klientów firmy w której pracuje.

Szkolenie odbywa się w formule BYOL (Bring Your Own Laptop). Wymagania: 8GB RAM, 5GB HDD oraz prawa admina! Laptop najlepiej by miał zainstalowane darmowe i dostępne na każdy system operacyjny programy: Burp Suite Community, Java 11, OWASP ZAP, JMeter, przeglądarki (polecamy Firefox i Chrome, tak, mogą przydać się obie, choć nieraz wystarczy jedna). Dla chętnych proponujemy VirtualBox z maszyną wirtualną z Kali Linuxem. Najistotniejsze są programy, z ich pomocą realizujemy laboratoria.

Informacje dodatkowe

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

https://niebezpiecznik.pl/szkolenia/bezpieczenstwo-w-testach-oprogramowania-dla-qa/?zai

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

Adres

ul. Armii Krajowej 11
30-150 Kraków
woj. małopolskie

Szczegóły miejsca realizacji usługi wysyłane są do Uczestników szkolenia na tydzień przed danym terminem.

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Lunch oraz przerwy kawowe w trakcie szkoleń stacjonarnych.

Kontakt

Magda Kowalska

E-mail szkolenia@niebezpiecznik.pl

Telefon (+48) 124 420 244