Możliwość dofinansowania

Niebezpiecznik.pl
Piotr Konieczny

★★★★★

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

Numer usługi 2025/02/07/148153/2547693

Kraków / stacjonarna
Usługa szkoleniowa
16 h
30.06.2025 do 01.07.2025

6 147,54 PLN brutto
4 998,00 PLN netto
384,22 PLN brutto/h
312,38 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	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	20-06-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	16
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 zawiera opis efektów uczenia się?

Certyfikat zawiera opis efektów uczenia.

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

Certyfikat zawiera informację, że walidacja została przeprowadzona w oparciu o kryteria weryfikacji tj. laboratoria przygotowane na symulowanym środowisku kształcenia.

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

Certyfikat zawiera informację o zastosowaniu rozwiązań metody walidacji jaką jest obserwacja w warunkach symulowanych.

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 przedmiotów/zajęć: 9

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Narzędzia deweloperskie przeglądarki oraz narzędzia typu lokalnego Proxy i ich wykorzystanie podczas testów bezpieczeństwa	Tomasz Borek	30-06-2025	09:00	11:00	02:00
2 z 9 Omówienie zakresu podstawowych testów bezpieczeństwa aplikacji webowych i web serwisów, najczęstszych podatności i sposobów ich wykrywania (z wykorzystaniem Burp Suite)	Tomasz Borek	30-06-2025	11:00	13:00	02:00
3 z 9 Bezpieczeństwo i użyteczność	Tomasz Borek	30-06-2025	13:00	15:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 9 Testy wydajnościowe z użyciem narzędzia JMeter w kontekście bezpieczeństwa	Tomasz Borek	30-06-2025	15:00	17:00	02:00
5 z 9 Automatyzacja testów bezpieczeństwa (z wykorzystaniem OWASP ZAP, Selenium Webdriver i Pythona)	Tomasz Borek	01-07-2025	09:00	11:00	02:00
6 z 9 Testy bezpieczeństwa jako element testów akceptacyjnych	Tomasz Borek	01-07-2025	11:00	13:00	02:00
7 z 9 Od testera do pentestera	Tomasz Borek	01-07-2025	13:00	15:00	02:00
8 z 9 Omówienie dokumentów	Tomasz Borek	01-07-2025	15:00	16:00	01:00
9 z 9 Podstawowe certyfikaty z zakresu testów bezpieczeństwa	Tomasz Borek	01-07-2025	16:00	17:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 147,54 PLN
Koszt przypadający na 1 uczestnika netto	4 998,00 PLN
Koszt osobogodziny brutto	384,22 PLN

Koszt osobogodziny netto	312,38 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

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