Możliwość dofinansowania

Łowca błędów - bug bounty dla początkujących

Numer usługi 2025/07/04/10671/2858266

3 013,50 PLN brutto
2 450,00 PLN netto
188,34 PLN brutto/h
153,13 PLN netto/h

Sages Spółka z ograniczoną odpowiedzialnością

4,4 / 5
288 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
23.10.2025 do 24.10.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie adresowane jest dla osób rozpoczynających przygodę z bug bounty, testerów, programistów, administratorów sieci, którzy chcą poznać inne spojrzenie na problemy bezpieczeństwa aplikacji
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	13-10-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Poznanie technik testowania bezpieczeństwa z perspektywy łowcy błędów

Nauka szybkiego wykrywania podatności w systemach i aplikacjach

Zrozumienie zagrożeń bezpieczeństwa istotnych dla dużych organizacji

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Poznanie technik testowania bezpieczeństwa z perspektywy łowcy błędów	Zrozumienie zagrożeń bezpieczeństwa istotnych dla dużych organizacji	Obserwacja w warunkach rzeczywistych
Nauka szybkiego wykrywania podatności w systemach i aplikacjach		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

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

Szkolenie będzie prowadzone zdalnie, w czasie rzeczywistym, na żywo, z trenerem, możliwością zadawania pytań.

Każdego dnia zajęcia w godz. 9:00-17:00, z przerwą na lunch około godz. 13:00

Podstawowe informacje o bug bounty

Omówienie przykładowych, prawdziwych raportów

Wykorzystanie narzędzi ffuf, nmap, amass, Caido, massdns

Techniki rekonesansu

Wykorzystanie list ładunków (payloadów) typu SecLists

Analiza Javascript

Sprytne wykrywanie błędów wstrzyknięć (XSS, SQLi itp.)

Wykrywanie ataków SSRF, XXE

Testowanie IDOR i błędów autoryzacji

Testowanie API

Testowanie uwierzytelniania, 2FA i JWT

Sprytne błędy logiki biznesowej i podatności w procesach np zakupowych

Łączenie podatności i podnoszenie priorytetu w celu zdobycia większej nagrody

Walidacja

Harmonogram

Liczba przedmiotów/zajęć: 4

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 4 Podstawowe informacje o bug bounty Omówienie przykładowych, prawdziwych raportów Wykorzystanie narzędzi ffuf, nmap, amass, Caido, massdns Techniki rekonesansu	Sebastian Chmielewski	23-10-2025	09:00	13:00	04:00
2 z 4 Wykorzystanie list ładunków (payloadów) typu SecLists Analiza Javascript Sprytne wykrywanie błędów wstrzyknięć (XSS, SQLi itp.)	Sebastian Chmielewski	23-10-2025	13:00	17:00	04:00
3 z 4 Wykrywanie ataków SSRF, XXE Testowanie IDOR i błędów autoryzacji Testowanie API Testowanie uwierzytelniania, 2FA i JWT	Sebastian Chmielewski	24-10-2025	09:00	13:00	04:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 4 Sprytne błędy logiki biznesowej i podatności w procesach np zakupowych Łączenie podatności i podnoszenie priorytetu w celu zdobycia większej nagrody	Sebastian Chmielewski	24-10-2025	13:00	17:00	04:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 013,50 PLN
Koszt przypadający na 1 uczestnika netto	2 450,00 PLN
Koszt osobogodziny brutto	188,34 PLN
Koszt osobogodziny netto	153,13 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Sebastian Chmielewski

Ekspert QA z ponad 12-letnim doświadczeniem, specjalizujący się w zapewnianiu bezpieczeństwa produktów oraz szeroko pojętym zapewnieniu jakości oprogramowania. Moje kompetencje obejmują automatyzację testów funkcjonalnych i wydajnościowych, testy penetracyjne, a także przeglądy kodu, co pozwala na identyfikację i eliminację potencjalnych zagrożeń już na najwcześniejszych etapach cyklu życia aplikacji. W trakcie mojej kariery osiągnąłem znaczące sukcesy w dziedzinie bug bounty – zgłosiłem 48 podatności w serwisie BugCrowd, co plasuje mnie na pozycji 650 w światowym rankingu na tej platformie. Zdobyłem certyfikaty OSWE (Offsec Web Expert) i OSED (Offsec Exploit Developer).

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

część teoretyczna szkolenia, slajdy - zostanie przekazana uczestnikom na szkoleniu w formie pdf.

uczestnik otrzyma certyfikat uczestnictwa z opisem nabytych umiejętności

Warunki uczestnictwa

Podstawowa znajomość sieci i aplikacji webowych

Podstawowa znajomość zagrożeń bezpieczeństwa (np. OWASP Top Ten, Portswigger Academy)

Umiejętność obsługi narzędzi takich jak przeglądarka czy terminal

Chęć do nauki i eksperymentowania

Informacje dodatkowe

Szkolenie będzie prowadzone zdalnie, w czasie rzeczywistym, na żywo, z trenerem, możliwością zadawania pytań.

Warunki techniczne

szkolenie na platformie zoom, wymagane:

stabilne połączenie internetowe (zalecane min. 10Mbit/s download i 1Mbit/s upload)

przeglądarka internetowa Chrome

zainstalowana aplikacja Zoom App

dobrej jakości słuchawki oraz mikrofon (opcjonalnie) kamera internetowa

link do szkolenia zostanie przesłany uczestnikom przed szkoleniem i będzie aktywny do końca szkolenia.

Kontakt

Agata Tuliszka-Kamińska

E-mail a.kaminska@sages.com.pl
Telefon (+48) 530 612 226