Możliwość dofinansowania

Szkolenie WEB-200 Web Attacks with Kali Linux - kompleksowy kurs e-learningowy

Numer usługi 2026/03/09/142469/3390854

7 870,77 PLN brutto
6 399,00 PLN netto
39,95 PLN brutto/h
32,48 PLN netto/h
196,00 PLN cena rynkowa

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,3 / 5

169 ocen

zdalna
Usługa szkoleniowa
197 h
30.04.2026 do 31.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Kurs WEB-200 Web Attacks with Kali Linux jest przeznaczony dla osób, które chcą zdobyć podstawowe umiejętności w zakresie profesjonalnej oceny aplikacji internetowych. Materiały szkoleniowe pomogą w zrozumieniu ataków i technik stosowanych przez cyberprzestępców przeciwko aplikacjom internetowym. Szkolenie w języku angielskim.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	1
Data zakończenia rekrutacji	17-04-2026
Forma prowadzenia usługi	zdalna
Liczba godzin usługi	197
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

Celem kursu jest przygotowanie uczestników do samodzielnego identyfikowania i eksploatowania powszechnych podatności aplikacji webowych przy wykorzystaniu narzędzi Kali Linux.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Opisuje typy luk w zabezpieczeniach typu Cross-Site Scripting (XSS)	Charakteryzuje główne typy ataków XSS	Test teoretyczny z wynikiem generowanym automatycznie
Opisuje metodę ataku SQL Injection	Opisuje technikę SQL Injection	Test teoretyczny z wynikiem generowanym automatycznie
	Identyfikuje punkty SQL Injection	Test teoretyczny z wynikiem generowanym automatycznie
	Opisuje techniki zapobiegania atakom typu SQL injection oraz metody ich łagodzenia.	Test teoretyczny z wynikiem generowanym automatycznie
Opisuje mechanizm Same-Origin	Wyjaśnia zasady Same-Origin i ich interakcję z żądaniami cross-origin	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje luki w zabezpieczeniach	Identyfikuje luki w zabezpieczeniach Cross-Origin Resource Sharing (CORS)	Test teoretyczny z wynikiem generowanym automatycznie
	Identyfikuje i wykorzystuje luki w zabezpieczeniach Cross-Site Request Forgery (CSRF)	Test teoretyczny z wynikiem generowanym automatycznie
Korzysta z narzędzi do testowania web aplikacji	Korzysta z narzędzi np. Burp Suite, Nmap, i Gobuster aby testować web aplikacje	Test teoretyczny z wynikiem generowanym automatycznie
Korzysta z narzędzi do wyszukiwania plików i katalogów.	Wyszukuje plik i katalogi za pomocą narzędzi takich jak Wfuzz i Hakrawler	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje ofensywne techniki JavaScript w celu wykorzystania luk w zabezpieczeniach aplikacji internetowych	Opisuje ofensywne techniki JavaScript	Test teoretyczny z wynikiem generowanym automatycznie
	Wykorzystuje ofensywne techniki JavaScript w celu wykorzystania luk w zabezpieczeniach aplikacji internetowych	Test teoretyczny z wynikiem generowanym automatycznie

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

Kurs **WEB-200 Web Attacks with Kali Linux** to kompleksowy kurs, który wprowadza w świat testowania bezpieczeństwa aplikacji webowych. Uczestnicy uczą się identyfikować i eksploatować powszechne podatności, takie jak XSS, CSRF, SQL Injection, SSRF, XXE, CORS czy SSTI, wykorzystując narzędzia Kali Linux. Kurs łączy teorię z praktyką poprzez realistyczne laboratoria i ćwiczenia, co pozwala na efektywne przyswajanie wiedzy.

Szkolenie realizowane jest w formule **e-learningu asynchronicznego** (self-paced) **w języku angielskim**.

Uczestnik otrzymuje dostęp do indywidualnie wygenerowanego konta **na platformie OffSec** na okres **90 dni.** W tym czasie może korzystać z materiałów bez narzuconych terminów i godzin nauki, dostosowując tempo oraz harmonogram nauki do własnej dyspozycyjności.

Walidacja: Na koniec usługi Uczestnik wykonuje post-test w celu dokonania oceny wzrostu poziomu wiedzy (test teoretyczny z wynikiem generowanym automatycznie).

Web Attacks with Kali Linux (WEB-200) e-learning

- 90 dni dostępu do kursu i laboratoriów praktycznych **na platformie OffSec**
- Jedno podejście do egzaminu certyfikacyjnego wliczone w cenę.
- Ponad 50 laboratoriów Proving Grounds Play – symulacje ataków w realistycznym środowisku.
- Bonusowy dostęp do kursu PEN-103, umożliwiający zdobycie dodatkowego certyfikatu.

Struktura szkolenia:

Kurs WEB-200 składa się **z ponad 16 modułów tematycznych**, obejmujących łącznie **197 godz**.

Każdy moduł tematyczny zawiera szczegółowe wyjaśnienia, studia przypadków i ćwiczenia praktyczne, mające na celu kładzenie nacisku na odkrywanie, testowanie i wykorzystywanie tych luk w celu doskonalenia umiejętności w zakresie bezpieczeństwa ofensywnego. Po ukończeniu modułów uczestnicy będą mogli sprawdzić swoją wiedzę wykonując laboratoria Challenge. Po przygotowaniu uczestnik może przystąpić do certyfikacji OffSec Web Assessor (OSWA).

Program szkolenia:

Narzędzia dla Web Assessor

Poznanie i praktyczne użycie standardowych narzędzi stosowanych przez pentesterów aplikacji webowych, aby sprawnie identyfikować i walidować podatności.

Cross-Site Scripting (XSS) — wprowadzenie, wykrywanie, eksploatacja i studium przypadku

Zrozumienie mechanizmów XSS, identyfikacja punktów wstrzyknięć, przeprowadzanie kontrolowanych testów w środowisku laboratoryjnym oraz omówienie sposobów ochrony aplikacji i użytkowników.

Cross-Site Request Forgery (CSRF)

Poznanie technik wykrywania podatności CSRF, symulacja ataków w bezpiecznych laboratoriach oraz wdrażanie i testowanie skutecznych zabezpieczeń przeciwko CSRF.

Wykorzystywanie błędnych konfiguracji CORS

Identyfikacja niewłaściwych ustawień CORS, ocena ryzyka związanego z niepoprawną polityką dostępu oraz rekomendacje konfiguracji zapobiegających wyciekom danych.

Enumeracja bazy danych

Nauka technik służących do wykrywania struktury i metadanych bazy danych aplikacji oraz metod ograniczania ujawniania wrażliwych informacji.

SQL Injection (SQLi)

Analiza i identyfikacja punktów podatnych na SQLi, bezpieczne testy eksploatacyjne w labie oraz techniki zapobiegania i hardenowania zapytań do bazy danych.

Directory Traversal

Wykrywanie i testowanie podatności na dostęp do chronionych zasobów przez manipulację ścieżkami oraz implementacja zabezpieczeń przed nieautoryzowanym dostępem do systemu plików.

XML External Entities (XXE)

Zrozumienie, jak błędna obsługa XML może prowadzić do wycieków lub wykonania kodu, oraz sposoby zabezpieczenia parserów XML i testowania aplikacji pod kątem XXE.

Server-Side Template Injection (SSTI)

Identyfikacja luk w mechanizmach renderowania szablonów po stronie serwera, praktyczne testy i metody neutralizacji zagrożeń wynikających z SSTI.

Server-Side Request Forgery (SSRF)

Poznanie wektorów SSRF, ocena skutków ataków umożliwiających dostęp do wewnętrznych zasobów i wdrożenie ograniczeń/filtrów zapobiegających SSRF.

Command Injection

Identyfikacja punktów wykonywania poleceń systemowych z poziomu aplikacji, kontrolowane testy i strategie zabezpieczania wejść oraz środowiska uruchomieniowego.

Insecure Direct Object Referencing (IDOR)

Wykrywanie problemów z bezpiecznym odwoływaniem się do zasobów (IDOR), ocena wpływu oraz projektowanie mechanizmów autoryzacji i kontroli dostępu zapobiegających nieautoryzowanym operacjom.

Składanie elementów: przegląd oceny aplikacji webowej

Łączenie poznanych technik i narzędzi w pełny proces audytu aplikacji webowej — od rozpoznania przez wykrywanie i weryfikację podatności po rekomendacje naprawcze i raportowanie.

Szkolenie przygotowuje do certyfikacji OSWA (OffSec Web Assessor Exam).

Egzamin OSWA (OffSec Web Assessor Exam)

- Egzamin praktyczny z bezpieczeństwa aplikacji webowych, potwierdzający zdolność do identyfikowania i eksploatowania podatności w aplikacjach internetowych w realistycznych warunkach.

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 870,77 PLN

Koszt przypadający na 1 uczestnika netto	6 399,00 PLN
Koszt osobogodziny brutto	39,95 PLN
Koszt osobogodziny netto	32,48 PLN

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- **90 dni** dostępu do kursu (materiały do pobrania w pdf. oraz materiały video) i laboratoriów praktycznych **na platformie OffSec**
- Jedno podejście do egzaminu certyfikacyjnego wliczone w cenę.
- Ponad 50 laboratoriów Proving Grounds Play – symulacje ataków w realistycznym środowisku.

Warunki uczestnictwa

Wymagana znajomość języka angielskiego na poziomie B1/B2 (średnio-zaawansowany)

Przed przystąpieniem do kursu zalecamy posiadanie podstawowych umiejętności związanych z systemem Linux, sieciami i tworzeniem skryptów, które będą bardzo pomocne w trakcie tego kursu.

Warunki techniczne

Realizacja za pomocą platformy e-learningowej OffSec https://portal.offsec.com

Wymagania sprzętowe:

- komputer z dostępem do internetu o minimalnej przepustowości 20Mb/s.

- wbudowane lub peryferyjne urządzenia do obsługi audio - słuchawki/głośniki oraz mikrofon.

- zainstalowana przeglądarka internetowa - Microsoft Edge/ Internet Explorer 10+ / **Google Chrome** 39+ (sugerowana) / Safari 7+

Kontakt

Ewa Kasprzak

E-mail ewa.kasprzak@softronic.pl
Telefon (+48) 618 658 840