



Hackuj strony i systemy: testy penetracyjne w praktyce

Numer usługi 2026/02/11/202247/3324539

3 444,00 PLN brutto
2 800,00 PLN netto
123,00 PLN brutto/h
100,00 PLN netto/h
261,33 PLN cena rynkowa ⓘ

JSYSTEMS SPÓŁKA
Z OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

Brak ocen dla tego dostawcy

- 📄 Usługa szkoleniowa
- 📺 zdalna w czasie rzeczywistym
- 🕒 28:00 h
- 📅 23.11.2026 do 26.11.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Dla osób technicznych, administratorów systemów, specjalistów IT i osób planujących rozpocząć karierę w pentestingu lub cyberbezpieczeństwie.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	19-11-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	28
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

Nabycie przez uczestników praktycznych umiejętności przeprowadzania testów penetracyjnych aplikacji webowych i systemów, umożliwiających samodzielne wykonywanie oceny bezpieczeństwa metodą etycznego hackingu, identyfikację podatności i tworzenie rekomendacji naprawczych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Przeprowadza rekonesans i zbieranie informacji o celu testu.	Uczestnik przeprowadza rekonesans pasywny i aktywny wskazanego zasobu testowego, dokumentując zebrane informacje (subdomeny, porty, usługi, technologie) przy użyciu odpowiednich narzędzi.	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje i exploituje podatności aplikacji webowych (OWASP Top 10). Przeprowadza testy bezpieczeństwa sieci i systemów.	Uczestnik identyfikuje i exploituje co najmniej 2 podatności (np. SQL Injection, XSS, IDOR) w środowisku laboratoryjnym, dokumentując wektor ataku i wpływ. Uczestnik wykonuje skanowanie podatności wskazanego hosta, identyfikuje otwarte porty i usługi oraz wskazuje co najmniej jedną podatność umożliwiającą dalszą eksploatację.	Test teoretyczny z wynikiem generowanym automatycznie Test teoretyczny z wynikiem generowanym automatycznie
Dokumentuje wyniki testów penetracyjnych i formułuje rekomendacje.	Uczestnik sporządza raport z testu penetracyjnego zawierający opis metodyki, wykaz podatności z klasyfikacją ryzyka (CVSS) i konkretne rekomendacje naprawcze.	Test teoretyczny z wynikiem generowanym automatycznie

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

1 dzień

1. Wprowadzenie

o Pentester, red teamer a może hacker?

☒ Kto to jest pentester?

☒ Kto to jest red teamer?

☒ Kto to jest hacker?

☒ Czym różnią się ich profesje?

o Czym są testy penetracyjne?

☒ Omówienie czym są testy penetracyjne

☒ Rodzaje testów penetracyjnych

☒ White Box

☒ Gray Box

☒ Black Box

o Czym się różni pentest web aplikacji od pentestu systemów operacyjnych?

☒ Omówienie zagadnienia

o Dlaczego testy penetracyjne są tak istotne?

☒ Omówienie zagadnienia

☒ Cyberataki

☒ Definicja cyberataku.

☒ Definicja podatności.

☒ Najpopularniejsze zagrożenia

☒ OWASPTOP10

☒ CWETOP25

☒ Otwarta dyskusja.

2. Standardy przeprowadzania testów penetracyjnych (i nie tylko)

o Czym jest standard bezpieczeństwa?

☒ Omówienie zagadnienia

o Omówienie różnic pomiędzy poszczególnymi standardami

☒ OWASP

☒ CIS

☒ PCI

☒ ISO

☒ Inne

☒ Który standard jest najlepszy i dlaczego?

☒ Otwarta dyskusja

☒ Który standard wybrać i dlaczego?

☒ Otwarta dyskusja

3. Narzędzia wykorzystywane podczas testów penetracyjnych

o Skanery podatności, które można wykorzystać do wstępnej analizy bezpieczeństwa badanego systemu operacyjnego:

☒ Nessus / Tenable / GVM

☒ NMAP

o Testy penetracyjne systemów operacyjnych

☒ Narzędzia, które można wykorzystać w systemach operacyjnych z rodziny Linux

☒ Lynis

☒ RkHunter

☒ Chkrootkit

☒ Ettercap

☒ Inne

☒ Narzędzia, które można wykorzystać w systemach operacyjnych z rodziny Windows

☒ Windows Security

☒ Microsoft PC Manager

☒ BloodHound

☒ GetIf

☒ RdpThief

☒ ADRecon

☒ LIZA

☒ Inne (gtworek repository)

2 dzień

4. Warsztaty praktyczne z zakresu pentestów systemów operacyjnych

o Jak w bezpieczny sposób można nauczyć się testów penetracyjnych systemów operacyjnych?

☒ Omówienie poszczególnych zestawów oprogramowania, które można wykorzystać do nauki testów penetracyjnych:

☒ Metasploitable

☒ DVL

☒ Vulnerable-AD

☒ Gameof Active Directory

☒ Escalate_Win

☒ Vulnerable_Machine

☒ Prezentacja zestawu wykorzystywanego podczas szkolenia;

☒ Pierwsze próby połączenia do maszyn szkoleniowych.

o Testowanie penetracyjne systemów operacyjnych w praktyce w oparciu o ciekawe narzędzia

☒ Wykorzystanie w praktyce "podstawowych" funkcjonalności narzędzi;

☒ Wykorzystanie w praktyce "zaawansowanych" funkcjonalności narzędzi.

o Propozycje poprawek.

☒ Omówienie zagadnienia

☒ Otwarta dyskusja

o Podsumowanie dnia warsztatowego

☒ Pytania i odpowiedzi

3 dzień

5. Testy penetracyjne web aplikacji

o Omówienie popularnych narzędzi i ich zastosowania:

☒ Burp Suite / ZAP

☒ Wireshark

☒ Sqlmap

☒ Metasploit

☒ Hydra

☒ John the Ripper

☒ Inne

6. Omówienie dodatków do przeglądarek internetowych wykorzystywanych przy testach penetracyjnych:

o OWASPPenetration Testing KIT

o Instant Data Scraper

o EditThisCookie

o Wappalyzer

o Shodan

o FoxyProxy

o Hack-Bar

o HackTools

o DotGit

7. Omówienie dystrybucji Linuxa przeznaczonych do testów penetracyjnych (i nie tylko):

o Kali Linux

o ParrotOS

o BlackArche

8. Podsumowanie zagadnień teoretycznych

o Krótkie podsumowanie zdobytej wiedzy

o Pytania i odpowiedzi

4 dzień

9. Warsztaty praktyczne z zakresu pentestów web aplikacji

o Jak w bezpieczny sposób można nauczyć się testów penetracyjnych web aplikacji?

☒ Omówienie poszczególnych zestawów oprogramowania, które można wykorzystać do nauki testów penetracyjnych:

☒ DVWA

☒ DVNA

☒ WebGoat

☒ Vulnerable-AD

☒ OWASPVulnerable Web Application

☒ Prezentacja zestawu wykorzystywanego podczas szkolenia;

☒ Pierwsze próby połączenia do maszyn szkoleniowych.

o Testowanie penetracyjne web aplikacji w praktyce w oparciu o najpopularniejsze podatności

☒ Wykorzystanie w praktyce "podstawowych" funkcjonalności narzędzi;

☒ Wykorzystanie w praktyce "zaawansowanych" funkcjonalności narzędzi.

o Tworzenie raportu po wykonanych testach penetracyjnych web aplikacji

☒ Elementy niezbędne do stworzenia poprawnego raportu z testów penetracyjnych web aplikacji:

☒ Tytuł

☒ Opis

☒ Komponent, którego dotyczy podatność.

☒ Potencjalna liczba użytkowników objętych podatnością.

☒ Krytyczność

☒ Wpływ

☒ Prawdopodobieństwo wystąpienia

☒ Pełne wyjaśnienie

☒ Ocena wskaźnika Common Vulnerability Scoring System

☒ Narzędzia użyte do wywołania podatności

☒ Kroki niezbędne do reprodukcji błędu.

☒ Sugerowane rozwiązanie

☒ Inne (CWE)

o Propozycje poprawek.

☒ Omówienie zagadnienia

☒ Otwarta dyskusja

o Podsumowanie szkolenia

☒ Pytania i odpowiedzi

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
-------------------	------------	-----------------------	---------------------	---------------------	---------------

Brak wyników.

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 444,00 PLN
Koszt przypadający na 1 uczestnika netto	2 800,00 PLN
Koszt osobogodziny brutto	123,00 PLN
Koszt osobogodziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Adrian Chaber

Trener posiada wieloletnie doświadczenie praktyczne w obszarze bezpieczeństwa aplikacji i testów penetracyjnych, przy czym kluczowe kwalifikacje w zakresie etycznego hackingu, testów penetracyjnych aplikacji webowych oraz identyfikacji podatności (OWASP Top 10) zostały zdobyte i są czynnie wykorzystywane w okresie ostatnich 5 lat (od 2021 roku do chwili obecnej). Potwierdzają to zrealizowane audyty bezpieczeństwa dla organizacji komercyjnych oraz przeprowadzone szkolenia z cybersecurity w latach 2022–2026.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Informacje o materiałach dla uczestników usługi - Uczestnicy otrzymają komplet materiałów PDF. Każdy uczestnik otrzymuje kod dostępu i

dane logowania do platformy ZOOM na 7 dni przed datą rozpoczęcia szkolenia. Dane przesyłane są na adres e-mail podany podczas rejestracji.

Warunki uczestnictwa

Podstawowa znajomość systemów operacyjnych (Linux i Windows), sieci komputerowych i działania aplikacji webowych. Umiejętność pracy z konsolą oraz chęć pracy warsztatowej. Umiejętność korzystania z komputera

Informacje dodatkowe

Warunkiem ukończenia szkolenia i otrzymania zaświadczenia jest uzyskanie minimalnej frekwencji na poziomie 80% całkowitego czasu trwania usługi. Obecność uczestnika będzie potwierdzana na podstawie codziennych list obecności lub logów z platformy online.

Warunki techniczne

Uczestnik musi dysponować sprzętem i łączem o parametrach:

- Procesor: min. 4-rdzeniowy (np. Intel i5/i7 lub odpowiednik AMD/M1/M2)
- Pamięć RAM: min. 16 GB
- Dysk: min. 20 GB wolnej przestrzeni
- System operacyjny: Windows 10/11 Pro, Linux lub macOS
- Multimedia: Sprawna kamera internetowa oraz mikrofon (wymagane do komunikacji i weryfikacji obecności)
- Łącze internetowe: Stabilne połączenie o minimalnej prędkości 10 Mbps (download) / 5 Mbps (upload)
- Oprogramowanie: Uprawnienia administratora pozwalające na instalację narzędzi

Kontakt



Biuro Obsługi Klienta

E-mail biuro@jssystemy.pl

Telefon (+48) 534 506 503