Możliwość dofinansowania

"FUNDACJA ETRP"

4,8 / 5

7 ocen

Szkolenie: Jak zostać hakerem? Pierwsze kroki w etycznym hakowaniu z Kali Linux. Rozdział 1-Testowanie bezpieczeństwa aplikacji webowych.

Numer usługi 2026/03/02/144863/3373419

Usługa szkoleniowa

zdalna w czasie rzeczywistym

20:00 h

12.10.2026 do 16.10.2026

5 000,00 PLN brutto

5 000,00 PLN netto

250,00 PLN brutto/h

250,00 PLN netto/h

332,00 PLN cena rynkowa

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Grupa docelowa usługi	Usługa skierowana jest do osób zainteresowanych tematyką bezpieczeństwa IT i aplikacji webowych, które chcą zdobyć praktyczne umiejętności z zakresu testów penetracyjnych na poziomie podstawowym lub średniozaawansowanym. W szczególności do: • specjalistów IT, helpdesk, administratorów i programistów, • studentów kierunków technicznych, chcących rozpocząć karierę w cyberbezpieczeństwie, • osób przygotowujących się do certyfikacji typu CEH, eJPT, OSCP (na poziomie wstępnym), • pracowników firm i instytucji chcących zwiększyć odporność aplikacji na ataki.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	11-10-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	20
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

Usługa przygotowuje do nabycia umiejętności w zakresie identyfikowania i testowania podatności aplikacji webowych zgodnie z wytycznymi OWASP Top 10 oraz zasadami etycznego hakowania. Uczestnik nauczy się przeprowadzać rekonesans, analizować luki w aplikacjach, wykorzystywać profesjonalne narzędzia (np. Burp Suite, ZAP Proxy) oraz raportować wyniki testów zgodnie z dobrymi praktykami bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje typowe podatności aplikacji webowych zgodnie z OWASP Top 10	Definiuje podatności i rozpoznaje ich skutki	Test teoretyczny
Opisuje działanie narzędzi Burp Suite i ZAP Proxy	Wymienia funkcje i możliwości użycia	Test teoretyczny
Przeprowadza rekonesans aplikacji webowej	Wykorzystuje WHOIS, Dirbuster, analizuje dane	Obserwacja w warunkach rzeczywistych
Wykonuje test podatności typu SQLi i XSS	Prezentuje skuteczne wykorzystanie i dokumentuje wynik	Obserwacja w warunkach rzeczywistych
Przechwytuje i modyfikuje żądania HTTP przy użyciu proxy	Pokazuje działający przykład ingerencji w żądanie	Obserwacja w warunkach rzeczywistych
Działa zgodnie z zasadami etycznego testowania	Nie testuje bez zgody, stosuje procedury zgłaszania luk	Test teoretyczny

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 4. Czy dokument potwierdzający uzyskanie kwalifikacji jest rozpoznawalny i uznawalny w danej branży/sektorze (czy certyfikat otrzymał pozytywne rekomendacje od co najmniej 5 pracodawców danej branży/sektorów lub związku branżowego, zrzeszającego pracodawców danej branży/sektorów)?

TAK

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa

Nazwa Podmiotu prowadzącego walidację	Design Center
Nazwa Podmiotu certyfikującego	Design Center

Program

Usługa prowadzona jest w godzinach dydaktycznych. Przerwy nie są wliczone w ogólny czas usługi rozwojowej. Harmonogram usługi może ulec nieznacznemu przesunięciu, ponieważ ilość przerw oraz długość ich trwania zostanie dostosowana indywidualnie do potrzeb uczestników szkolenia. Łączna długość przerw podczas szkolenia nie będzie dłuższa aniżeli zawarta w harmonogramie.

Szczegółowy harmonogram realizacji usługi zostanie dostosowany do potrzeb i możliwości uczestników a jego finalna wersja zostanie podana zgodnie z wymaganiami systemu BUR, przed rozpoczęciem realizacji usługi.

Zajęcia zostaną przeprowadzone przez ekspertów z wieloletnim doświadczeniem, którzy przekazuje nie tylko wiedzę teoretyczną, ale także praktyczne wskazówki i najlepsze praktyki. Uczestnicy mają możliwość czerpania z jego wiedzy i doświadczeń.

Moduł 1: Wprowadzenie do bezpieczeństwa aplikacji webowych i OWASP Top 10 (2 godziny)

- Wprowadzenie do etycznego hakowania
- Struktura aplikacji webowej (HTTP, sesje, ciasteczka)
- OWASP Top 10 – przegląd najczęstszych podatności

Moduł 2: Rekonesans i analiza aplikacji webowych (3 godziny)

- Pasywny i aktywny rekonesans (Whois, DNSdump, SSLscan)
- Wykorzystanie narzędzi Dirbuster, Gobuster, Nmap
- Analiza struktury aplikacji i enumeracja punktów wejścia

Moduł 3: Ataki na aplikacje – SQL Injection, XSS, CSRF (5 godzin)

- Testowanie ręczne i automatyczne SQLi
- Wstrzykiwanie JavaScript – ataki refleksyjne i trwałe (XSS)
- CSRF i zabezpieczenia typu token / SameSite
- Ćwiczenia w środowiskach testowych (DVWA, Juice Shop)

Moduł 4: Burp Suite i ZAP Proxy – przechwytywanie i manipulowanie ruchem (3 godziny)

- Konfiguracja proxy i przeglądarki
- Przechwytywanie żądań i odpowiedzi
- Modyfikowanie payloadów, automatyzacja testów
- Skanowanie aktywne i pasywne

Moduł 5: Zaawansowane scenariusze i logika aplikacji (3 godziny)

- Bypassowanie uwierzytelniania (brute-force, sesje, JWT)
- Logiczne błędy w aplikacjach – case study
- Przykłady luk w uprawnieniach, kolejności działań, parametrach

Moduł 6: Raportowanie i etyka testów (2 godziny)

- Responsible disclosure – jak zgłaszać luki
- Elementy dobrego raportu z testów penetracyjnych
- Ograniczenia prawne i etyczne w testowaniu

Walidacja (1 godzina)

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	5 000,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	250,00 PLN
Koszt osobogodziny netto	250,00 PLN
W tym koszt walidacji brutto	120,00 PLN
W tym koszt walidacji netto	120,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Paweł Pudo

Od ponad pięciu lat Paweł Pudo intensywnie rozwija kompetencje w obszarach cyberbezpieczeństwa, administracji IT oraz edukacji cyfrowej, z powodzeniem łącząc umiejętności techniczne z talentem do klarownego przekazywania wiedzy nietechnicznym odbiorcom. Obecnie odpowiada za całość infrastruktury IT w jednostce edukacyjnej, gdzie zarządza m.in. środowiskiem sieciowym, Azure Active Directory, pakietem Office 365, drukiem 3D i administracją stron internetowych. Równocześnie prowadzi audyty zgodne z normami ISO/IEC 27001:2017-06, ISO

22301:2020-04 oraz RODO, wspierając instytucje w budowaniu bezpiecznych i zgodnych z przepisami systemów informatycznych. Ukończył kurs audytora wiodącego SZBI (ISO 27001). Paweł od lat prowadzi szkolenia z zakresu cyberbezpieczeństwa dla szkół, samorządów i przedsiębiorstw, dzieląc się praktyczną wiedzą i doświadczeniem. Znany z wyjątkowej umiejętności tłumaczenia skomplikowanych zagadnień technicznych w prosty i przystępny sposób, co czyni go niezwykle skutecznym edukatorem i konsultantem. W 2021 roku ukończył studia podyplomowe "Bezpieczeństwo i ochrona cyberprzestrzeni" na Uniwersytecie Ekonomicznym w Katowicach. W ostatnim czasie intensywnie szkoli się również w zakresie zastosowań sztucznej inteligencji w edukacji i biznesie, wykorzystując AI m.in. do budowania narzędzi szkoleniowych. Regularnie występuje jako prelegent na wydarzeniach branżowych, dzieląc się wiedzą jako członek społeczności cybersec.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Informacje o materiałach dla uczestników usługi

Uczestnik otrzyma skrypt, materiały dydaktyczne w formie prezentacji oraz zestaw ćwiczeń w formie cyfrowej- pdf.

Warunki uczestnictwa

Warunki uczestnictwa:

- Podstawowa znajomość obsługi komputera, przeglądarek internetowych i systemu operacyjnego (Windows lub Linux).
- Podstawowa wiedza z zakresu działania sieci komputerowych i protokołu HTTP.
- Umiejętność pracy z edytorem tekstu i terminalem systemowym (cmd/bash).
- Własny komputer z dostępem do Internetu, możliwością instalacji oprogramowania oraz uprawnieniami administratora.
- Zainstalowana przeglądarka internetowa (np. Firefox, Chrome)
- Chęć pracy w środowiskach testowych i respektowania zasad etycznego testowania bezpieczeństwa.

Informacje dodatkowe

Podstawa zwolnienia z VAT:

1) art. 43 ust. 1 pkt 29 lit. c Ustawy z dnia 11 marca 2024 o podatku od towarów i usług - w przypadku dofinansowania w wysokości 100%

2) § 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 dofinansowania w co najmniej 70%

3) W przypadku braku uzyskania dofinansowania lub uzyskania dofinansowania poniżej 70%, do ceny usługi należy doliczyć 23% VAT

Warunki techniczne

Szkolenie realizowane jest w czasie rzeczywistym za pośrednictwem platformy wideokonferencyjnej (Click Meeting).

Uczestnik powinien dysponować:

- komputerem/laptopem z min. 4 GB RAM, procesorem x64 (zalecane: 8 GB RAM i SSD),
- systemem operacyjnym umożliwiającym uruchomienie **maszyny wirtualnej (np. VirtualBox)** lub środowiska **Kali Linux (VM/Live USB)**,
- stabilnym łączem internetowym (min. 10 Mb/s),
- przeglądarką internetową (zalecany: Chrome/Firefox),
- aktywnym mikrofonem i kamerą (wymagane),

Kontakt

ARIEL BANASZEWSKI

E-mail szkolenia@fundacjaetrp.pl

Telefon (+48) 22 1627 981