Możliwość dofinansowania

Dagma sp. z o.o.

Techniki hackingu i cyberprzestępczości - Strony WWW i aplikacje webowe - poziom 2

Numer usługi 2025/05/22/17164/2763610

zdalna w czasie rzeczywistym
Usługa szkoleniowa
21 h
23.07.2025 do 25.07.2025

4 590,00 PLN brutto
4 590,00 PLN netto
218,57 PLN brutto/h
218,57 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 przeznaczone jest dla osób pracujących w sektorze IT, spełniających poniższe wymagania: • Znajomość podstaw Linuxa, działania sieci, zasady działania systemów • Wiedza ze szkolenia **Techniki hackingu i cyberprzestępczości - Etyczny Hacking w praktyce - poziom 1**
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	15-07-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	21
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 skutecznego rozpoznawania ataków na aplikacje webowe i strony www oraz przeciwdziałaniu metodom atakowania i włamywania się do systemów informatycznych przez luki w oprogramowaniu www, w związku z czym uczestnik jest w stanie w pełni zabezpieczyć systemy operacyjne oraz sieci informatyczne swojej firmy.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik stosuje i broni się przed nowoczesnymi technikami internetowych włamywaczy;	Uczestnik zabezpiecza systemy operacyjne oraz sieci informatyczne	Obserwacja w warunkach symulowanych
Uczestnik samodzielnie rozpoznaje ataki na aplikacje webowe i strony www	Uczestnik dobiera właściwe metody ochrony przed cyberatakami	Obserwacja w warunkach symulowanych
Uczestnik nabędzie kompetencje społeczne, takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.	Projektuje działania w oparciu o zasady empatii, budowania zaufania i efektywnej komunikacji	Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Tak, dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się.

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

Tak, dokument stanowi potwierdzenie, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

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

Tak, dokument potwierdza, że zostały zastosowane rozwiązania zapewniające rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Moduł 1 Wprowadzenie do tematyki ataków na strony internetowe i aplikacje webowe - zajęcia teoretyczne (wykład)

- Głębokie ukrycie

Moduł 2 Insecure Logins Forms - zajęcia teoretyczne (wykład)

- Logout Management

Moduł 3 Password Attack - zajęcia praktyczne (ćwiczenia)

- Account Lockout

Moduł 4 Web Parameter Tampering - zajęcia praktyczne (ćwiczenia)

- Path oraz Information Disclosure

Moduł 5 Path Traversal - zajęcia teoretyczne (wykład)

- Local File Inclusion

Moduł 6 Remote File Inclusion - zajęcia praktyczne (ćwiczenia)

- Omijanie filtrowania danych

Moduł 7 Command Injection (+ Blind) - zajęcia teoretyczne (wykład)

- Sessions Management

Moduł 8 Upload File - zajęcia praktyczne (ćwiczenia)

- CSRF - Cross Site Request Forgery

Moduł 9 SQL Injection - GET, POST - zajęcia praktyczne (ćwiczenia)

- XSS Attack - Reflected, Stored
- Automatyzacja SQL Injection
- **WALIDACJA**

Razem 21 godzin lekcyjnych, (15 godzin i 45 minut zegarowych).

- - Walidacja jest wliczona w czas trwania szkolenia.
  - Przerwy nie są wliczone w czas trwania szkolenia

Harmonogram

Liczba przedmiotów/zajęć: 10

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 Moduł 1 Wprowadzenie do tematyki ataków na strony internetowe i aplikacje webowe - zajęcia teoretyczne (wykład)	Armand Pajor	23-07-2025	09:00	10:30	01:30
2 z 10 Moduł 2 Insecure Logins Forms - zajęcia teoretyczne (wykład)	Armand Pajor	23-07-2025	10:45	13:00	02:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 10 Moduł 3 Password Attack - zajęcia praktyczne (ćwiczenia)	Armand Pajor	23-07-2025	13:30	15:00	01:30
4 z 10 Moduł 4 Web Parameter Tampering - zajęcia praktyczne (ćwiczenia)	Armand Pajor	24-07-2025	09:00	10:30	01:30
5 z 10 Moduł 5 Path Traversal - zajęcia teoretyczne (wykład)	Armand Pajor	24-07-2025	10:45	13:00	02:15
6 z 10 Moduł 6 Remote File Inclusion - zajęcia praktyczne (ćwiczenia)	Armand Pajor	24-07-2025	13:30	15:00	01:30
7 z 10 Moduł 7 Command Injection (+ Blind) - zajęcia teoretyczne (wykład)	Armand Pajor	25-07-2025	09:00	10:30	01:30
8 z 10 Moduł 8 Upload File - zajęcia praktyczne (ćwiczenia)	Armand Pajor	25-07-2025	10:45	13:00	02:15
9 z 10 Moduł 9 SQL Injection - GET, POST - zajęcia praktyczne (ćwiczenia)	Armand Pajor	25-07-2025	13:30	14:40	01:10
10 z 10 Walidacja	-	25-07-2025	14:40	15:00	00:20

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 590,00 PLN
Koszt przypadający na 1 uczestnika netto	4 590,00 PLN
Koszt osobogodziny brutto	218,57 PLN
Koszt osobogodziny netto	218,57 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Armand Pajor

Doświadczenie zawodowe: Trener IT, prowadzący szkolenia w Dagma Szkolenia IT od początku 2023 roku. Wdrożeniowiec i analityk cyberbezpieczeństwa sieci. Prowadzący autorskie szkolenie firmy FORSEC z zakresu Technik hackingu oraz Cyberbezpieczeństwa sieci (Lan Security Analyst) i systemów operacyjnych (OS Security Analyst)
Uzyskane certyfikacje: ITIL Foundation Certificate in IT Service Management, Corporate Readiness Certificate - Information Security Management, Corporate Readiness Certificate - Troubleshooting
Specjalizacja: Sieci komputerowe, Cyberbezpieczeństwo, Network Traffic Analysis, Cyber Threat Hunting (CTH), C#, Python, Java
Wykształcenie: wyższe, Politechnika Krakowska, magister Informatyki
Posiada doświadczenie w prowadzeniu tego typu szkoleń (w ciągu 2 lat przeprowadził 21 szkoleń dla łącznej grupy ok.176 osób)

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- - materiały dydaktyczne w formie elektronicznej (link do materiałów producenta lub e-book, lub dostęp do materiałów autorskich, przygotowanych przez trenera, przesłane na adres e-mail uczestnika)
  - dostęp do przygotowanego środowiska wirtualnego na czas szkolenia

Warunki uczestnictwa

Warunkiem otrzymania dofinansowania jest spełnienie warunków przedstawionych przez Operatora, który jest dysponentem funduszy publicznych w Państwa regionie. Do Operatora składają Państwo dokumenty o dofinansowanie do usługi rozwojowej.

Cena obejmuje szkolenie objęte dofinansowaniem w wysokości przynajmniej 70%. Podstawą do zastosowania stawki zwolnionej jest dokonanie płatności przez Operatora całości bądź części podlegającej finansowaniu **w innym przypadku do podanej ceny netto należy doliczyć 23% VAT.**

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową https://szkolenia.dagma.eu/pl w celu rezerwacji miejsca.

Informacje dodatkowe

Informacje organizacyjne:

- - Jedna godzina lekcyjna to 45 minut
  - W cenę szkolenia nie wchodzą koszta związane z dojazdem, wyżywieniem oraz noclegiem.
  - Uczestnik otrzyma zaświadczenie DAGMA Szkolenia IT o ukończeniu szkolenia
  - Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej (na wniosku reklamacyjnym) i odsyłając na adres szkolenia@dagma.pl. Reklamacja zostaje rozpatrzona do 30 dni od dnia otrzymania dokumentu przez DAGMA Sp. z o.o.
  - Podstawa zwolnienia z VAT: dofinansowanie w co najmniej 70% - zgodnie z treścią § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20.12.2013r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2013 r. poz. 1722 ze zm.)

Warunki techniczne

WARUNKI TECHNICZNE:

a) platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa:

- **ZOOM i/lub MS Teams**
- w przypadku kilku uczestników przebywających w jednym pomieszczeniu, istnieją dwie możliwości udziału w szkoleniu:

1) każda osoba bierze udział w szkoleniu osobno (korzystając z oddzielnych komputerów), wówczas należy wyciszyć dźwięki z otoczenia by uniknąć sprzężeń;

2) otrzymujecie jedno zaproszenie, wówczas kilka osób uczestniczy w szkoleniu za pośrednictwem jednego komputera

- Można łatwo udostępniać sobie ekran, oglądać pliki, bazę handlową, XLS itd.

b) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

- Uczestnik potrzebuje komputer z przeglądarką Chrome lub Edge (NIE firefox), mikrofon, głośniki.

c) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:

- łącze internetowe o przepustowości minimum 10Mbit,

d) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów:

- uczestnik na tydzień przed szkoleniem otrzyma maila organizacyjnego, ze szczegółową instrukcją pobrania darmowej platformy ZOOM.
- Z platformy MS Teams można korzystać za pośrednictwem przeglądarki, nie trzeba nic instalować.

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie: https://szkolenia.dagma.eu/pl/technical-requirements

Kontakt

Agnieszka Palenga

E-mail palenga.a@dagma.pl

Telefon (+48) 32 7931 139