Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2020/2021

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma sudiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo

1 Informacje o przedmiocie

Nazwa przedmiotu	Bezpieczeństwo aplikacji internetowych
Nazwa przedmiotu w języku angielskim	Security of the Web Services and Applications
Kod przedmiotu	WIiT I oIIS D3 20/21
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	4.00
Semestry	1

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
1	30	0	30	0	0	0

3 Cele przedmiotu

Cel 1 Zapoznanie z podstawowymi technikami ataków na aplikacje internetowe i Web Servicy oraz możliwościami ich wykrywania.

Cel 2 Zapoznanie z dostępnymi narzędziami do testowania bezpieczeństwa webaplikacji.

Cel 3 Zrozumienie współczesnych problemów bezpieczeństwa aplikacji i usług internetowych.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Podstawowa wiedza z zakresu programowania, szczególnie programowania aplikacji internetowych.

2 Umiejętność projektowania i implementacji algorytmów i prostych struktur danych.

3 Podstawowa wiedza z zakresu systemów operacyjnych i kryptografii.

5 Efekty kształcenia

EK1 Wiedza Zna i rozumie podstawowe metody, techniki i narzędzia informatyczne stosowane do wykrywania zagrożeń i ataków na aplikacje i usługi internetowe.

EK2 Wiedza Posiada zaawansowaną wiedzę na temat mechanizmów umożliwiających zabezpieczenie systemów webowych przed atakami.

EK3 Umiejętności Potrafi analizować systemy webowe pod kątem bezpieczeństwa, wykrywać ich podatności na ataki oraz zabezpieczać je przed nimi.

EK4 Umiejętności Potrafi przeprowadzić eksperymenty w zakresie symulowania skutecznych ataków na webaplikacje.

EK5 Kompetencje społeczne Umie pracować indywidualnie i w grupie oraz przekazywać uzyskane rezultaty pracy w zrozumiały sposób.

6 Treści programowe

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Organizacja zajęć, omówienie programu ćwiczeń laboratoryjnych, konfiguracja sprzętu, zapoznanie się z systemem Kali Linux.	2
L2	Symulacja ataku HTTP Parameter Pollution.	2
L3	Symulacje ataków na aplikacje i usługi internetowe.	6
L4	Symulacje ataków na bazę danych.	6
L5	Symulacje ataków na sesję.	6
L6	Filtrowanie danych wejściowych w aplikacjach internetowych.	2
L7	Ochrona przed spamem w systemach internetowych.	2
L8	Stosowanie certyfikatu SSL.	2
L9	Praca własna studentów, podsumowanie zajęć i ocena pracy studentów.	2

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Ogólny model bezpieczeństwa aplikacji internetowych, web serviceów, baz danych oraz wpływ wykorzystywanych komponentów na bezpieczeństwo systemu.	2
W2	Przegląd narzędzi automatyzujących wykrywanie podatności aplikacji internetowych na ataki.	2
W3	Współczesne problemy bezpieczeństwa aplikacji i usług internetowych.	2
W4	Różne praktyki tworzenia aplikacji internetowych i ich wpływ na bezpieczeństwo, dokumenty OWASP.	2
W5	Ograniczenia aplikacji po stronie klienta, problemy przeglądarek.	4
W6	Typowe ataki na aplikacje webowe.	4
W7	Ataki na bazę danych.	4
W8	Ataki na sesje.	4
W9	Filtrowanie danych w aplikacjach webowych jako mechanizm bezpieczeństwa.	2
W10	Ochrona przed spamem.	2
W11	Protokół SSL i jego funkcja w zakresie bezpieczeństwa webaplikacji.	2

7 Narzędzia dydaktyczne

N1 Wykłady

N2 Ćwiczenia laboratoryjne

N3 Prezentacje multimedialne

N4 Konsultacje

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	60
Konsultacje przedmiotowe	8
Egzaminy i zaliczenia w sesji	4
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	20
Opracowanie wyników	14
Przygotowanie raportu, projektu, prezentacji, dyskusji	14
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**120**
Sumaryczna liczba punktów ECTS dla przedmiotu	4.00

9 Sposoby oceny

Ocena formująca

F1 Ćwiczenia praktyczne

F2 Wejściówki

F3 Sprawozdania z ćwiczeń laboratoryjnych

Ocena podsumowująca

P1 Średnia ważona ocen formujących

P2 Egzamin pisemny

Warunki zaliczenia przedmiotu

W1 Pozytywna ocena z ćwiczeń praktycznych i wejściówek

W2 Obecność na co najmniej 50% zajęć laboratoryjnych

W3 Pozytywna ocena z egzaminu

Ocena aktywności bez udziału nauczyciela

B1 Sprawozdanie z ćwiczenia laboratoryjnego

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 3.0	Student zna i rozumie podstawowe zagadnienia związane z bezpieczeństwem aplikacji webowych.
Efekt kształcenia 2	
Na ocenę 3.0	Student posiada podstawową wiedzę na temat zabezpieczenia aplikacji internetowych przed atakami.
Efekt kształcenia 3	
Na ocenę 3.0	Student potrafi analizować systemy webowe pod kątem bezpieczeństwa i zabezpieczać je przed najbardziej popularnymi atakami.
Efekt kształcenia 4	
Na ocenę 3.0	Student potrafi przeprowadzić ataki XSS oraz SQL Injection.
Efekt kształcenia 5	
Na ocenę 3.0	Student w miarę sumiennie uczęszcza na zajęcia, radzi sobie z pracą indywidualna.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	I2_W02 I2_W03 I2_W05 I2_W08	Cel 1 Cel 2 Cel 3	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11	N1 N3 N4	P1 P2
EK2	I2_W02 I2_W03 I2_W05 I2_W08	Cel 2 Cel 3	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11	N1 N3 N4	P1 P2
EK3	I2_U01b I2_U02b I2_U07 I2_U11 I2_U12	Cel 2 Cel 3	L2 L3 L4 L5 L6 L7 L8	N2 N3 N4	F1 F2 F3

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK4	I2_U01b I2_U02b I2_U07 I2_U11 I2_U12	Cel 1 Cel 3	L2 L3 L4 L5	N2 N3 N4	F1 F2 F3
EK5	I2_K03 I2_K04	Cel 3	L1 L2 L3 L4 L5 L6 L7 L8 L9	N2 N3 N4	F1 F2 F3

11 Wykaz literatury

Literatura podstawowa

[1] P. Prasad — *Testy penetracyjne nowoczesnych serwisów. Kompendium inżynierów bezpieczeństwa*, , 2017, Helion

[2] P. Kim — *Podręcznik pentestera. Bezpieczeństwo systemów informatycznych*, , 2015, Helion

Literatura uzupełniająca

[1] M. Bentkowski, A. Czyż, R. Janicki, J. Kamiński, A. Maichalczyk, M. Niezabitowski, M. Piosek, M. Sajdak, G. Trawiński, B. Widła — *Bezpieczeństwo aplikacji webowych*, , 2019, Securitum Szkolenia sp. z o.o. sp.k.

[2] P. Hope, B. Walther — *Testowanie bezpieczeństwa aplikacji internetowych. Receptury*, , 2010, Helion

[3] R. Messier — *Kali Linux. Testy bezpieczeństwa, testy penetracyjne i etyczne hakowanie*, , 2019, Helion

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr Adam Marszałek (kontakt: amarszalek@pk.edu.pl)

Osoby prowadzące przedmiot

1 mgr inż. Andrzej Wilczyński (kontakt: andrzej.wilczynski@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .