Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2021/2022

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 21/22
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.	10
L4	Symulacje ataków na bazę danych.	6
L5	Symulacje ataków na sesję.	6
L8	Symulacje ataków na protokół SSL.	2
L9	Praca własna studentów, podsumowanie zajęć i ocena pracy studentów.	2

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin

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 iich wpływ na bezpieczeństwo - dokumenty OWASP.	2
W5	Typowe ataki na aplikacje webowe.	8
W6	Ataki na bazy danych.	4
W7	Ataki na sesje.	4
W8	Problemy przeglądarek, bezpieczeństwo protokołu HTTP/2.	4
W9	Protokół SSL, systemy IDS, IPS i WAF.	2

7 Narzędzia dydaktyczne

N1 Wykłady (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

N2 Ćwiczenia laboratoryjne (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

N3 Prezentacje multimedialne (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

N4 Konsultacje (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

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 Egzamin pisemny sprawdzający wiedzę z wykładów

F2 Wejściówki i kolokwia na laboratoriach

F3 Ćwiczenia praktyczne na laboratoriach

Ocena podsumowująca

P1 Średnia ważona ocen formujących

Warunki zaliczenia przedmiotu

W1 Pozytywna ocena z egzaminu pisemnego z wykładu

W2 Pozytywna ocena z zajęć laboratoryjnych (wejściówki, kolokwia, ćwiczenia praktyczne)

W3 Obecność na co najmniej 50% zajęć laboratoryjnych

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.

Na ocenę 3.0	Student opanował co najmniej 50% materiału.
Na ocenę 3.5	Student opanował więcej niż 60% materiału.
Na ocenę 4.0	Student opanował więcej niż 70% materiału.
Na ocenę 4.5	Student opanował więcej niż 80% materiału.
Na ocenę 5.0	Student opanował więcej niż 90% materiału.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
Na ocenę 3.0	Student opanował co najmniej 50% materiału.
Na ocenę 3.5	Student opanował więcej niż 60% materiału.
Na ocenę 4.0	Student opanował więcej niż 70% materiału.
Na ocenę 4.5	Student opanował więcej niż 80% materiału.
Na ocenę 5.0	Student opanował więcej niż 90% materiału.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
Na ocenę 3.0	Student opanował co najmniej 50% materiału.
Na ocenę 3.5	Student opanował więcej niż 60% materiału.
Na ocenę 4.0	Student opanował więcej niż 70% materiału.
Na ocenę 4.5	Student opanował więcej niż 80% materiału.
Na ocenę 5.0	Student opanował więcej niż 90% materiału.
Efekt kształcenia 4	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
Na ocenę 3.0	Student opanował co najmniej 50% materiału.
Na ocenę 3.5	Student opanował więcej niż 60% materiału.
Na ocenę 4.0	Student opanował więcej niż 70% materiału.
Na ocenę 4.5	Student opanował więcej niż 80% materiału.
Na ocenę 5.0	Student opanował więcej niż 90% materiału.
Efekt kształcenia 5	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.

Na ocenę 3.0	Student opanował co najmniej 50% materiału.
Na ocenę 3.5	Student opanował więcej niż 60% materiału.
Na ocenę 4.0	Student opanował więcej niż 70% materiału.
Na ocenę 4.5	Student opanował więcej niż 80% materiału.
Na ocenę 5.0	Student opanował więcej niż 90% materiału.

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	N1 N3 N4	F1
EK2	I2_W02 I2_W03 I2_W05 I2_W08	Cel 2 Cel 3	W1 W2 W3 W4 W5 W6 W7 W8 W9	N1 N3 N4	F1
EK3	I2_U01b I2_U02b I2_U07 I2_U11 I2_U12	Cel 2 Cel 3	L1 L2 L3 L4 L5 L8 L9	N2 N3 N4	F2 F3
EK4	I2_U01b I2_U02b I2_U07 I2_U11 I2_U12	Cel 1 Cel 3	L1 L2 L3 L4 L5 L8 L9	N2 N3 N4	F2 F3
EK5	I2_K03 I2_K04	Cel 3	L1 L2 L3 L4 L5 L8 L9	N2 N3 N4	F2 F3

11 Wykaz literatury

Literatura podstawowa

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

Literatura uzupełniająca

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

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

Osoby prowadzące przedmiot

1 dr 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)

. . . . . .