

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2019/2020

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo dla licencjatów

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 19/20
KATEGORIA PRZEDMIOTU	Przedmioty specjalnościowe
LICZBA PUNKTÓW ECTS	4.00
SEMESTRY	2

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	SEMINARIUM	PROJEKT
2	30	0	30	0	0	0

3 CELE PRZEDMIOTU

Cel 1 Zapoznanie z podstawowymi technikami ataków na aplikacje internetowe i Web Services 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 weba-plikacje.
- 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	Usługi internetowe jako narzędzie do wymiany danych.	3
L3	Symulacje ataków na aplikacje i usługi internetowe.	6
L4	Symulacje ataków na bazę danych.	5
L5	Symulacje ataków na sesję.	5
L6	Filtrowanie danych wejściowych w aplikacjach internetowych.	3
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	Współczesne problemy bezpieczeństwa aplikacji i usług internetowych.	3
W2	Przegląd narzędzi automatyzujących wykrywanie podatności aplikacji internetowych na ataki.	3
W3	Różne praktyki tworzenia aplikacji internetowych i ich wpływ na bezpieczeństwo, dokumenty OWASP.	2
W4	Ograniczenia aplikacji po stronie klienta, problemy przeglądarek.	2
W5	Ogólny model bezpieczeństwa aplikacje internetowe, web services, bazy danych, wpływ wykorzystywanych komponentów na bezpieczeństwo systemu.	2
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	2
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	20
Opracowanie wyników	10
Przygotowanie raportu, projektu, prezentacji, dyskusji	20
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 Ćwiczenie praktyczne

F2 Wejściówka

F3 Sprawozdanie z ćwiczenia laboratoryjnego

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 2.0	Opanowanie nie więcej niż 50% materiału.
NA OCENĘ 3.0	Opanowanie więcej niż 50% materiału.
NA OCENĘ 3.5	Opanowanie więcej niż 60% materiału.
NA OCENĘ 4.0	Opanowanie więcej niż 70% materiału.
NA OCENĘ 4.5	Opanowanie więcej niż 80% materiału.
NA OCENĘ 5.0	Opanowanie więcej niż 90% materiału.
EFEKT KSZTAŁCENIA 2	
NA OCENĘ 2.0	Opanowanie nie więcej niż 50% materiału.
NA OCENĘ 3.0	Opanowanie więcej niż 50% materiału.
NA OCENĘ 3.5	Opanowanie więcej niż 60% materiału.
NA OCENĘ 4.0	Opanowanie więcej niż 70% materiału.
NA OCENĘ 4.5	Opanowanie więcej niż 80% materiału.
NA OCENĘ 5.0	Opanowanie więcej niż 90% materiału.
EFEKT KSZTAŁCENIA 3	
NA OCENĘ 2.0	Opanowanie nie więcej niż 50% materiału.
NA OCENĘ 3.0	Opanowanie więcej niż 50% materiału.
NA OCENĘ 3.5	Opanowanie więcej niż 60% materiału.
NA OCENĘ 4.0	Opanowanie więcej niż 70% materiału.
NA OCENĘ 4.5	Opanowanie więcej niż 80% materiału.
NA OCENĘ 5.0	Opanowanie więcej niż 90% materiału.
EFEKT KSZTAŁCENIA 4	
NA OCENĘ 2.0	Opanowanie nie więcej niż 50% materiału.
NA OCENĘ 3.0	Opanowanie więcej niż 50% materiału.
NA OCENĘ 3.5	Opanowanie więcej niż 60% materiału.
NA OCENĘ 4.0	Opanowanie więcej niż 70% materiału.
NA OCENĘ 4.5	Opanowanie więcej niż 80% materiału.
NA OCENĘ 5.0	Opanowanie więcej niż 90% materiału.

EFEKT KSZTAŁCENIA 5	
NA OCENĘ 2.0	Opanowanie nie więcej niż 50% materiału.
NA OCENĘ 3.0	Opanowanie więcej niż 50% materiału.
NA OCENĘ 3.5	Opanowanie więcej niż 60% materiału.
NA OCENĘ 4.0	Opanowanie więcej niż 70% materiału.
NA OCENĘ 4.5	Opanowanie więcej niż 80% materiału.
NA OCENĘ 5.0	Opanowanie 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	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	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	L3 L4 L5 L6 L7 L8	N2 N3 N4	F1 F2 F3
EK4	I2_U01b I2_U02b I2_U05 I2_U07 I2_U11 I2_U12	Cel 1 Cel 3	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*, , 2019, Helion

LITERATURA UZUPEŁNIAJĄCA

- [1] **P. Hope, B. Walther** — *Testowanie bezpieczeństwa aplikacji internetowych. Receptury*, , 2012, Helion
- [2] **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 mgr. inż. Andrzej Wilczyński (kontakt: andrzej.wilczynski@pk.edu.pl)

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejsowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....