KARTA PRZEDMIOTU DLA NABORU 2020/2021

INFORMACJE OGÓLNE

1. **Nazwa przedmiotu kształcenia**
   BEZPIECZEŃSTWO APLIKACJI WEBOWYCH I MOBILNYCH
2. **Nazwa jednostki prowadzącej moduł** Zakład Informatyki
3. **Grupa treści kształcenia** -
4. **Typ przedmiotu** obowiązkowy
5. **Poziom studiów** pierwszego stopnia
6. **Liczba punktów ECTS** 2
7. **Poziom przedmiotu** średnio zaawansowany
8. **Rok studiów, semestr** III rok, semestr V
9. **Liczba godzin w semestrze** wykład 15h, laboratorium 30h
10. **Język wykładowy:** polski
11. **Wykładowca (wykładowcy)**

INFORMACJE SZCZEGÓŁOWE

12. Wymagania wstępne

1) Podstawy programowania WWW i aplikacji mobilnych
2) Podstawowa wiedza z bezpieczeństwa systemów komputerowych

13. Cele przedmiotu

C1 zdobywanie wiedzy w zakresie tworzenia bezpiecznych aplikacji webowych i mobilnych

C2 nabycie umiejętności analizy aplikacji webowych i mobilnych pod kątem bezpieczeństwa

C3 poznanie narzędzi ułatwiających wykrycie ataków na aplikacje webowe i mobilne

14. Efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych

Student, który zaliczył przedmiot potrafi:	odniesienie do kierunkowych efektów uczenia się
WIEDZA	
EU01 Student zna i rozumie podstawowe zagadnienia związane z bezpieczeństwem aplikacji webowych i mobilnych.	I1P_W05 I1P_W20 I1P_W21
EU02 Student posiada wiedzę dotyczącą tworzenia bezpiecznych aplikacji webowych i mobilnych	
UMIEJĘTNOŚCI	
EU03 Student umie analizować systemy webowe i mobilne pod kątem bezpieczeństwa.	I1P _U25 I1P _U30
EU04 Student posiada umiejętność przeprowadzenia testów odporności systemów webowych i mobilnych na ataki z wykorzystaniem różnych technik.	
EU05 Student jest w stanie zabezpieczać systemu webowe i mobilne przed popularnymi rodzajami ataków.	
KOMPETENCJE SPOŁECZNE	
EU06 Student jest świadomy ryzyk związanych nieodpowiednim zabezpieczeniem systemów webowych i mobilnych	I1P_K01 I1P_K04
EU07 Student umie współpracować w zespole w celu wypracowania jak najbezpieczniejszych systemów informatycznych	
EU08 Student rozumie, że wiedza i umiejętności z zakresu bezpieczeństwa aplikacji mobilnych i webowych stają się bardzo szybko nieaktualne	

15. Treści programowe

Forma zajęć – wykłady

Współczesne problemy bezpieczeństwa aplikacji webowych i mobilnych: zagrożenia wynikające z architektury aplikacji webowych i mobilnych oraz z technologii realizacji.
Dobre praktyki realizacji aplikacji webowych i mobilnych. Braki w zabezpieczeniach. Najważniejsze zagrożenia. Standardy zabezpieczania aplikacji internetowych (OWASP).
Ataki na aplikacje webowe i mobilne i zabezpieczanie się przed nimi. Mechanizmy obronne, testy penetracyjne. Przegląd narzędzi automatyzujących wykrywanie podatności na atak.

Forma zajęć – laboratoria

Współczesne problemy bezpieczeństwa aplikacji webowych i mobilnych: zagrożenia wynikające z architektury aplikacji webowych i mobilnych oraz z technologii realizacji.
Dobre praktyki realizacji aplikacji webowych i mobilnych.
Przykładowe ataki na aplikacje webowe i mobilne i zabezpieczanie się przed nimi (ataki typu injection, brute force, XSS, tapjacking itp.). Analiza rodzajów ataków na urządzenia pracujące na takich platformach, tj. Android, iOS i Windows
Analiza aplikacji i identyfikowanie problemów bezpieczeństwa.
Przegląd narzędzi automatyzujących wykrywanie podatności na atak.
Typowe podatności aplikacji mobilnych. Testy bezpieczeństwa aplikacji mobilnych (Android, iOS)
Mechanizmy obronne w aplikacjach dla poszczególnych platform, zabezpieczanie aplikacji niezależnych od platformy.

16. Narzędzia/metody dydaktyczne

1. Samodzielna praca nad projektem przy wsparciu prowadzącego
2. Prezentacja projektu

17. Sposoby oceny (F – formująca; P – podsumowująca)

F1. Kolokwium zaliczeniowe.

F2. Aktywność na zajęciach.

P1. Egzamin w formie pisemnej sprawdzający wiedzę z wykładów i laboratoriów

18. Obciążenia pracą studenta

forma aktywności	średnia liczba godzin na zrealizowanie aktywności
Kontakt z nauczycielem *	30+15
Nakład pracy studenta	
Samodzielna praca studenta	20
SUMA	65
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	2

19. Literatura podstawowa i uzupełniająca

Literatura dobierana indywidualnie do tematu projektu
Literatura podstawowa:

1) Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych Zasady i praktyka Tom 1, Helion 2018.
2) Kim P.: Podręcznik pentestera. Bezpieczeństwo systemów informatycznych, Helion 2015.
3) Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych Zasady i praktyka Tom 2, Helion 2019.

Literatura uzupełniająca:

1) PRASHANT VERMA, AKSHAY DIXIT, BEZPIECZEŃSTWO URZĄDZEŃ MOBILNYCH. RECEPTURY, Helion 2017
2) Chell D., Erasmus T. i in.: Bezpieczeństwo aplikacji mobilnych. Podręcznik hakera, Helion 2015.

20. Formy oceny - szczegóły

Warunki uzyskania zaliczenia przedmiotu: zajęcia kończą się egzaminem
Sposób weryfikacji efektów uczenia się:

Ocena stopnia osiągniętych przez studenta efektów uczenia się następuje wg poniższych kryteriów:
5.0 – zakładany efekt uczenia się został osiągnięty bez zastrzeżeń
4.5 – zakładany efekt uczenia się został osiągnięty z pojedynczymi brakami/błędami
4.0 – zakładany efekt uczenia się został osiągnięty z nielicznymi brakami/błędami
3.5 – zakładany efekt uczenia się został osiągnięty z wieloma brakami/błędami
3.0 – zakładany efekt kształcenia został osiągnięty z licznymi i istotnymi brakami/błędami (minimalnie wymagany poziom osiągnięcia efektu)

21. Inne przydatne informacje o przedmiocie

1. Bezpośrednich informacji o problematyce zajęć i treściach programowych udziela Prowadzący w trakcie zajęć i podczas konsultacji
2. Zajęcia odbywać się będą w PSW w Białej Podlaskiej
3. Konsultacje odbywać się będą zgodnie z obowiązującym terminarzem

* Zajęcia prowadzone z bezpośrednim udziałem nauczyciela akademickiego lub innej osoby prowadzącej zajęcia oraz konsultacje