SYLABUS

DOTYCZY CYKLU KSZTAŁCENIA 2025/26-2028/29

ROK AKADEMICKI 2026/27

1. PODSTAWOWE INFORMACJE O PRZEDMIOCIE

Nazwa przedmiotu	*Cyberbezpieczeństwo*
Kod przedmiotu*	
Nazwa jednostki prowadzącej kierunek	*Instytut Informatyki, Wydział Nauk Ścisłych i Technicznych*
Nazwa jednostki realizującej przedmiot	*Instytut Informatyki, Wydział Nauk Ścisłych i Technicznych*
Kierunek studiów	*Informatyka i ekonometria*
Poziom studiów	*studia pierwszego stopnia*
Profil	*praktyczny*
Forma studiów	*studia stacjonarne*
Rok i semestr/y studiów	*rok II, sem. IV*
Rodzaj przedmiotu	*przedmiot kierunkowy*
Język wykładowy	*polski*
Koordynator	*dr inż. Marcin Ochab*
Imię i nazwisko osoby prowadzącej / osób prowadzących	*dr inż. Marcin Ochab*

1.1. Formy zajęć dydaktycznych, wymiar godzin i punktów ECTS

Semestr (nr)	Wykł.	Ćw.	Konw.	Lab.	Sem.	ZP	Prakt.	Inne (jakie?)	**Liczba pkt. ECTS**
4	15			15					2

1.2. Sposób realizacji zajęć

☒ zajęcia w formie tradycyjnej

☐ zajęcia realizowane z wykorzystaniem metod i technik kształcenia na odległość

1.3. Forma zaliczenia przedmiotu (z toku) (egzamin, zaliczenie z oceną, zaliczenie bez oceny)

Zaliczenie z oceną

2.WYMAGANIA WSTĘPNE

Wiedza i umiejętności weryfikowane na przedmiotach: technologie internetowe, sieci komputerowe, programowanie obiektowe, bazy danych

3. CELE, EFEKTY UCZENIA SIĘ, TREŚCI PROGRAMOWE I STOSOWANE METODY DYDAKTYCZNE

3.1. Cele przedmiotu

C1	Zapoznanie z podstawowymi zagadnieniami związanymi z bezpieczeństwem informacji i systemów informatycznych.
C2	Zapoznanie się z najpopularniejszymi podatnościami występującymi głównie w aplikacjach internetowych i systemach bazodanowych.
C3	Zapoznanie się z metodami zapobiegania podatnościom występującym głównie w aplikacjach internetowych i systemach bazodanowych, oraz ich realizacją w celu utworzenia zabezpieczeń.
C4	Kształtowanie świadomości potrzeby ciągłego kształcenia się w obszarze bezpieczeństwa informatycznego

3.2. Efekty uczenia się dla przedmiotu

EK (efekt uczenia się)	Treść efektu uczenia się zdefiniowanego dla przedmiotu Student:	Odniesienie do efektów kierunkowych
EK_01	Zna najpopularniejsze zagrożenia dla aplikacji webowych oraz ich klasyfikacje.	K_W02
EK_02	Wykorzystuje podstawowe narzędzia do testowania bezpieczeństwa aplikacji oraz uwarunkowania prawne dotyczące ich stosowania.	K_U11, K_K03
EK_03	Zna zalecenia dotyczące budowania bezpiecznych aplikacji i umie ocenić ryzyko płynące braku ich implementacji.	K_W02, K_W05, K_U02
EK_04	Umie wykonać udokumentować przeprowadzone testy.	K_U07
EK_05	Umie dobrać odpowiednie narzędzia do testowania danych klas podatności.	K_U04, K_U07

3.3. Treści programowe

A. Problematyka wykładu

Uwarunkowania prawne dotyczące testowania bezpieczeństwa aplikacji
Istniejące klasyfikacje błędów dotyczących bezpieczeństwa aplikacji
Najpopularniejsze błędy w aplikacjach webowych na podstawie OWASP Top 10
Mechanizmy JWT, CORS, HSTS, nagłówki HTTP mające wpływ na bezpieczeństwo, serializacja
Hashowanie i idea Rainbow Tables, Authenticated Encryption
Sanityzacja danych po stronie frontend i backend
Przykłady podatności typu Injection (SQLi, Blind SQLi, XSS, OS command, XML)
Podstawowe zagadnienia OSINT

B. Problematyka laboratoriów

Konfiguracja maszyn wirtualnych potrzebnych do realizacji laboratorium.
Podatność SQL Injection (SQLi) – manualne i automatyczne sprawdzanie występowania podatności, przykładowe wykorzystanie podatności, realizacja zabezpieczeń na poziomie aplikacji internetowej i bazy danych.
Podatność Cross-site scripting (XSS) – manualne sprawdzanie występowania podatności, przykładowe wykorzystanie podatności, realizacja zabezpieczeń na poziomie aplikacji internetowej.
Podatność CSRF (Cross-Site Request Forgery) – manualne sprawdzanie występowania podatności, przykładowe wykorzystanie podatności, realizacja zabezpieczeń na poziomie aplikacji internetowych.

3.4. Metody dydaktyczne

Wykład: wykład z prezentacją multimedialną

Laboratorium: wykonywanie zadań praktycznych przy komputerze i sprawozdanie, informatyczny projekt praktyczny

4. METODY I KRYTERIA OCENY

4.1. Sposoby weryfikacji efektów uczenia się

Symbol efektu	Metody oceny efektów uczenia się (np.: kolokwium, egzamin ustny, egzamin pisemny, projekt, sprawozdanie, obserwacja w trakcie zajęć)	Forma zajęć dydaktycznych (w, ćw, ...)
ek_ 01	Kolokwium zaliczeniowe , sprawozdanie z ćwiczeń laboratoryjnych	lab
Ek_02	Kolokwium zaliczeniowe , sprawozdanie z ćwiczeń laboratoryjnych	lab
EK_03	Kolokwium zaliczeniowe , sprawozdanie z ćwiczeń laboratoryjnych	lab
EK_04	Kolokwium zaliczeniowe , sprawozdanie z ćwiczeń	lab

	laboratoryjnych	
EK_05	Kolokwium zaliczeniowe , sprawozdanie z ćwiczeń laboratoryjnych	lab

4.2. Warunki zaliczenia przedmiotu (kryteria oceniania)

Kryteria oceny:

Dla każdego efektu uczenia się:

- 3.0 – otrzymanie 50-59% punktów z zadań praktycznych przypisanych do efektu uczenia się.
- 3.5 – otrzymanie 60-69% punktów z zadań praktycznych przypisanych do efektu uczenia się.
- 4.0 – otrzymanie 70-79% punktów z zadań praktycznych przypisanych do efektu uczenia się.
- 4.5 – otrzymanie 80-89% punktów z zadań praktycznych przypisanych do efektu uczenia się.
- 5.0 – otrzymanie 90-100% punktów z zadań praktycznych przypisanych do efektu uczenia się.

Ocena końcowa jest średnią arytmetyczną ocen cząstkowych za każdy efekt uczenia się pod warunkiem, że wszystkie oceny cząstkowe są ocenami pozytywnymi.

Zasady uzyskania oceny końcowej:

Zaliczenie z laboratorium przedmiotu odbywa się na podstawie oceny z wykonanych sprawozdań z ćwiczeń laboratoryjnych oraz kolokwium. W ocenie uwzględniona jest terminowość oddania oraz stopień dokładności i poprawności wykonania sprawozdań.

Zaliczenie z wykładu na podstawie zaliczenia laboratorium

5. CAŁKOWITY NAKŁAD PRACY STUDENTA POTRZEBNY DO OSIĄGNIĘCIA ZAŁOŻONYCH EFEKTÓW W GODZINACH ORAZ PUNKTACH ECTS

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny z harmonogramu studiów	30
Inne z udziałem nauczyciela akademickiego (udział w konsultacjach, egzaminie)	
Godziny niekontaktowe – praca własna studenta (przygotowanie do zajęć, egzaminu, napisanie referatu itp.)	30
SUMA GODZIN	60
SUMARYCZNA LICZBA PUNKTÓW ECTS	2

6. PRAKTYKI ZAWODOWE W RAMACH PRZEDMIOTU

wymiar godzinowy	----
zasady i formy odbywania praktyk	----

7. LITERATURA

Literatura podstawowa:

1) Michał Bentkowski, Gynvael Coldwind, Artur Czyż, Rafał Janicki, Jarosław Kamiński, Adrian Michalczyk, Mateusz Niezabitowski, Marcin Piosek, Michał Sajdak, Grzegorz Trawiński, Bohdan Widła: *Bezpieczeństwo aplikacji webowych*, SECURITUM, 2019
2) Bezpieczeństwo nowoczesnych aplikacji internetowych : przewodnik po zabezpieczeniach / Andrew Hoffman ; przekład: Joanna Zatorska. - Gliwice : Helion, © 2021.
3) Bernardo Damele A. G. , Miroslav Stampar: *sqlmap user's manual*, 2011 - https://owasp.org/www-community/attacks/Blind_SQL_Injection

Literatura uzupełniająca:

1) https://sekurak.pl/czym-jest-sql-injection/
2) https://sekurak.pl/czym-jest-xss/
3) https://sekurak.pl/do-czego-mozna-wykorzystac-xss-czyli-czym-jest-beef/
4) https://sekurak.pl/czym-jest-podatnosc-csrf-cross-site-request-forgery/

5) https://sekurak.pl/czym-jest-cors-cross-origin-resource-sharing-i-jak-wplywa-na-bezpieczenstwo/
6) https://sekurak.pl/hsts-czyli-http-strict-transport-security/
7) https://sekurak.pl/php-object-injection-malo-znana-krytyczna-klasa-podatnosci/
8) https://sekurak.pl/owasp-top-ten-2021-a04-insecure-design-przeglad-przypadkow/
9) https://sekurak.pl/jak-w-prosty-sposob-zwiekszyc-bezpieczenstwo-aplikacji-webowej/

Akceptacja Kierownika Jednostki lub osoby upoważnionej