

SYLABUS

DOTYCZY CYKLU KSZTAŁCENIA 2021-2025

Rok akademicki 2024/2025

1. PODSTAWOWE INFORMACJE O PRZEDMIOCIE

Nazwa przedmiotu	<i>bezpieczeństwo systemów komputerowych</i>
Kod przedmiotu*	
nazwa jednostki prowadzącej kierunek	<i>Kolegium Nauk Przyrodniczych</i>
Nazwa jednostki realizującej przedmiot	<i>Kolegium Nauk Przyrodniczych</i>
Kierunek studiów	<i>informatyka</i>
Poziom studiów	<i>studia I stopnia</i>
Profil	<i>ogólnoakademicki</i>
Forma studiów	<i>stacjonarne</i>
Rok i semestr/ly studiów	<i>rok IV, semestr 7</i>
Rodzaj przedmiotu	<i>inżynierski przedmiot kierunkowy</i>
Język wykładowy	<i>język polski</i>
Koordynator	<i>dr inż. Marcin Ochab</i>
Imię i nazwisko osoby prowadzącej / osób prowadzących	<i>dr inż. Marcin Ochab, mgr inż. Jaromir Sarzyński</i>

* -opcjonalnie, zgodnie z ustaleniami w Jednostce

1.1. Formy zajęć dydaktycznych, wymiar godzin i punktów ECTS

Semestr (nr)	Wykł.	Ćw.	Konw.	Lab.	Sem.	ZP	Prakt.	Inne (jakie?)	Liczba pkt. ECTS
7	10			20					3

1.2. Sposób realizacji zajęć

zajęcia w formie tradycyjnej

1.3 Forma zaliczenia przedmiotu (z toku)

zaliczenie z oceną

2. WYMAGANIA WSTĘPNE

Wiedza i umiejętności weryfikowane na przedmiotach: systemy operacyjne, sieci komputerowe, algorytmy i struktury danych, programowanie obiektowe, aplikacje internetowe.

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

3.1 Cele przedmiotu

C ₁	Zapoznanie z podstawowymi zagadnieniami związanymi z bezpieczeństwem informacji i systemów informatycznych.
C ₂	Zapoznanie się z najpopularniejszymi podatnościami występującymi głównie w aplikacjach internetowych i systemach bazodanowych.
C ₃	Zapoznanie się z metodami zapobiegania podatnościom występującym głównie w aplikacjach internetowych i systemach bazodanowych oraz ich realizacją w celu utworzenia zabezpieczeń.
C ₄	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	Odniesienie do efektów kierunkowych ¹
EK_01	Zna najpopularniejsze zagrożenia dla aplikacji webowych i ich klasyfikacje oraz zalecenia dotyczące budowania bezpiecznych aplikacji. Zna podstawowe narzędzia do testowania bezpieczeństwa aplikacji oraz uwarunkowania prawne dotyczące ich stosowania.	K_Wo3, K_Wo4, K_Wo7, K_Wo8
EK_02	Potrafi ocenić ryzyko płynące z występowania wybranej podatności w aplikacji internetowej. Potrafi wybrać prawidłowe podejścia oraz sposoby realizacji zabezpieczeń zapobiegającym podatnościom.	K_U07, K_U20
EK_03	Potrafi udokumentować przeprowadzane sprawdzenia występowania wybranych podatności w aplikacjach internetowych. Potrafi zrealizować zabezpieczenia im zapobiegające.	K_U13, K_U16, K_U21

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'u i backend'u
Przykłady podatności typu Injection (SQLi, Blind SQLi, XSS, OS command, XML)
Podstawowe zagadnienia OSINT

¹ W przypadku ścieżki kształcenia prowadzącej do uzyskania kwalifikacji nauczycielskich uwzględnić również efekty uczenia się ze standardów kształcenia przygotowującego do wykonywania zawodu nauczyciela.

B. Problematyka ćwiczeń laboratoryjnych

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

3.4 Metody dydaktyczne

Wykład: wykład z prezentacją multimedialną,

Ćwiczenia laboratoryjne: wykonywanie zadań praktycznych przy komputerze.

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	wykład
EK_02	kolokwium	laboratorium
EK_03	sprawozdanie z ćwiczeń laboratoryjnych	laboratorium

4.2 Warunki zaliczenia przedmiotu (kryteria oceniania)

Zaliczenie z wykładu uzyskiwane jest na podstawie kolokwium.

Efekt EK_01 uznany jest za zaliczony, gdy student odpowie poprawnie na przynajmniej połowę przypisanych do niego pytań.

Zaliczenie z laboratorium uzyskiwane jest na podstawie:

- kolokwium,
- sprawozdań z ćwiczeń laboratoryjnych.

Ocena końcowa z laboratorium wystawiana jest na podstawie oceny uzyskanej z kolokwium.

Efekt EK_02 jest oceniany w skali 2.0 – 5.0 w ramach kolokwium, gdzie student wykonuje przypisane do niego zadania. Ocena przyznawana jest proporcjonalnie za uzyskany procent punktów do zdobycia. Efekt jest uznany za zaliczony, gdy student otrzyma ocenę przynajmniej dostateczny (za uzyskanie przynajmniej 50% punktów).

Efekt EK_03 uznany jest za zaliczony, jeśli student wykona wszystkie ćwiczenia laboratoryjne i udokumentuje je w formie sprawozdań.

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

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe wynikające 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.)	45
SUMA GODZIN	75
SUMARYCZNA LICZBA PUNKTÓW ECTS	3

* Należy uwzględnić, że 1 pkt ECTS odpowiada 25-30 godzin całkowitego nakładu pracy studenta.

6. PRAKTYKI ZAWODOWE W RAMACH PRZEDMIOTU

wymiar godzinowy	–
zasady i formy odbywania praktyk	–

7. LITERATURA

Literatura podstawowa: <ol style="list-style-type: none">1) Michał Bentkowski, Gynvael Coldwind, Artur Czyż, Rafał Janicki, Jarosław Kamiński, Adrian Michalczyk, Mateusz Niezabitowski, Marcin Piosek, Michał Sajdak, Grzegorz Trawiński, Bohdan Widła: <i>Bezpieczeństwo aplikacji webowych</i>, SECURITUM, 20192) Andrew Hoffman: <i>Bezpieczeństwo nowoczesnych aplikacji internetowych. Przewodnik po zabezpieczeniach</i>, Gliwice, Helion, 2021.3) Malcolm McDonald: <i>Bezpieczeństwo aplikacji internetowych dla programistów. Rzeczywiste zagrożenia, praktyczna ochrona</i>, Gliwice, Helion, 2021.4) Bernardo Damele A. G. , Miroslav Stampar: <i>sqlmap user's manual</i>, 2011
Literatura uzupełniająca: <ul style="list-style-type: none">• https://owasp.org/www-community/attacks/Blind_SQL_Injection• https://sekurak.pl/czym-jest-sql-injection/• https://sekurak.pl/czym-jest-podatnosc-csrf-cross-site-request-forgery/• https://sekurak.pl/czym-jest-cors-cross-origin-resource-sharing-i-jak-wplywa-na-bezpieczenstwo/• https://sekurak.pl/hsts-czyli-http-strict-transport-security/• https://sekurak.pl/owasp-top-ten-2021-a04-insecure-design-przeglad-przypadkow/• https://sekurak.pl/jak-w-prosty-sposob-zwiekszy-bezpieczenstwo-aplikacji-webowej/