Załącznik nr 1.5 do Zarządzenia Rektora UR nr 12/2019

SYLABUS

DOTYCZY CYKLU KSZTAŁCENIA *2020-2024*

Rok akademicki 2023/2024

1. PODSTAWOWE INFORMACJE O PRZEDMIOCIE

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

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

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	Odniesienie do efektów kierunkowych
EK_01	Zna najpopularniejsze zagrożenia dla aplikacji webowych i ich klasyfikacje oraz zalecenia dotyczące budowania bezpiecznych aplikacji.	K_W03, K_W04
EK_02	Zna podstawowe narzędzia do testowania bezpieczeństwa aplikacji oraz uwarunkowania prawne dotyczące ich stosowania.	K_W07, K_W08
EK_03	Umie ocenić ryzyko płynące z występowania podatności w aplikacji internetowej oraz zrealizować zabezpieczenia im zapobiegające.	K_U07, K_U13
EK_04	Umie udokumentować przeprowadzane sprawdzenia występowania wybranych podatności w aplikacjach internetowych.	K_U16
EK_05	Umie zaplanować i przeprowadzić test penetracyjny podatności w aplikacji internetowej przy użyciu dostępnych narzędzi.	K_U20, 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

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
EK_01	zaliczenie w formie testu	wykład
EK _02	zaliczenie w formie testu	wykład
EK _03	kolokwium	laboratorium
EK _04	sprawozdanie z ćwiczeń laboratoryjnych	laboratorium
EK _05	kolokwium	laboratorium

4.2 Warunki zaliczenia przedmiotu (kryteria oceniania)

Zaliczenie z wykładu uzyskiwane jest na podstawie testu.
Efekty EK_01 i EK_02 są oceniane jako „zal"/„nzal", uznane są za zaliczone, gdy student odpowie poprawnie na przynajmniej połowę pytań przypisanych do każdego z nich.

Zaliczenie z laboratorium uzyskiwane jest na podstawie: kolokwium, sprawozdań z ćwiczeń laboratoryjnych. Ocena końcowa z przedmiotu wystawiana jest na podstawie oceny uzyskanej z pierwszej części kolokwium.

Efekt EK_05 jest oceniany w skali 2.0 – 5.0 w ramach pierwszej części, gdzie student wykonuje przypisane do niego zadania praktyczne. Ocena przyznawana jest proporcjonalnie za uzyskany procent punktów do zdobycia w tej części. Efekt jest uznany za zaliczony, gdy student otrzyma ocenę przynajmniej dostateczny (za uzyskanie przynajmniej 50% punktów).
Efekt EK_04 uznany jest za zaliczony, jeśli student wykona wszystkie ćwiczenia laboratoryjne i udokumentuje je w formie sprawozdań.

Efekt EK_03 jest oceniany jako „zal"/„nzal" w ramach drugiej części kolokwium, gdzie student wykonuje przypisane do niego zadania praktyczne/ udziela odpowiedzi na pytania. Efekt

uznany jest za zaliczony, jeśli student uzyska przynajmniej połowę punktów możliwych do zdobycia w tej części.

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.)	45
SUMA GODZIN	75
SUMARYCZNA LICZBA PUNKTÓW ECTS	3

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) Andrew Hoffman: *Bezpieczeństwo nowoczesnych aplikacji internetowych. Przewodnik po zabezpieczeniach*, Gliwice, Helion, 2021.
3) Malcolm McDonald: *Bezpieczeństwo aplikacji internetowych dla programistów. Rzeczywiste zagrożenia, praktyczna ochrona*, Gliwice, Helion, 2021.
4) Bernardo Damele A. G. , Miroslav Stampar: *sqlmap user's manual*, 2011

Literatura uzupełniająca:

- 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-zwiekszyc-bezpieczenstwo-aplikacji-webowej/

Akceptacja Kierownika Jednostki lub osoby upoważnionej