Załącznik nr 1.5 do Zarządzenia Rektora UR nr 7/2023

SYLABUS

DOTYCZY CYKLU KSZTAŁCENIA *2023-2027*
Rok akademicki 2024/2025 i 2025/2026

1. PODSTAWOWE INFORMACJE O PRZEDMIOCIE

Nazwa przedmiotu	*cyberbezpieczeństwo*
Kod przedmiotu*	
nazwa jednostki prowadzącej kierunek	*Instytut Informatyki, Kolegium Nauk Przyrodniczych*
Nazwa jednostki realizującej przedmiot	*Instytut Informatyki, Kolegium Nauk Przyrodniczych*
Kierunek studiów	*informatyka*
Poziom studiów	*studia I stopnia*
Profil	*ogólnoakademicki*
Forma studiów	*stacjonarne*
Rok i semestr/y studiów	*rok II i III, semestr 4 i 5*
Rodzaj przedmiotu	*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*

***** *-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**
4	15			15					2
5	15			15					2

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 1, 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.
C5	Zapoznanie się z typowymi niestandardowymi technikami uzyskiwania zdalnego dostępu do systemów informatycznych.
C6	Poznanie narzędzi pozwalających na analizę stanu bezpieczeństwa systemu.

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_W02, K_W05, K_W08
EK_02	Potrafi ocenić ryzyko płynące z występowania wybranej podatności w aplikacji internetowej. Potrafi wybrać prawidłowe podejścia oraz sposoby realizacji zabezpieczeń zapobiegającym podatnościom.	K_U05, K_U06
EK_03	Jest gotów do podjęcia dialogu odnośnie cyberbezpieczeństwa oraz uświadamiania rozmówców na temat najpopularniejszych zagrożeń dotyczących aplikacji internetowych.	K_K02
EK_04	Zna typowe niestandardowe możliwości uzyskania dostępu do systemu operacyjnego. Zna narzędzia pozwalające na wykonanie rekonesansu. Zna sposoby typowe sposoby nawiązywania komunikacji z maszynami w sieci wewnętrznej. Zdaje sobie sprawę z potrzeby odpowiedniej złożoności haseł i stosowanych algorytmów.	K_W02, K_W05, K_W08

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

EK_05	Potrafi wykorzystać typowe niestandardowe możliwości uzyskania dostępu do systemu operacyjnego. Potrafi dobrać odpowiednie narzędzia rekonesansu zależnie od potrzeby i ich użyć. Potrafi nawiązać połączenie do sieci wewnętrznej pomimo prostego firewalla. Potrafi ocenić w praktyce czas potrzebny na złamanie hasła lub algorytmu.	K_U05, K_U06

3.3 Treści programowe

A. Problematyka wykładu

Część 1 (semestr 4)
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,
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
Część 2 (semestr 5)
Pasywny i aktywny rekonesans na przykładzie narzędzi: Shodan, nmap, dnsrecon, dnsenum , fuff, gobuster, onesixtyone, smbmap, snmpwalk, wpscan, OpenVAS, Nessus
Uzyskiwanie dostępu do linii komend za pomocą SSH, RDP, RPC, WinRM, webshell, meterpreter, reverseshell
Przekierowanie portów, tunelowanie i komunikacja z sieciami wewnętrznymi za pomocą narzędzi: SSH, socks, Plink, Netsh, proxychains oraz protokołów HTTP i DNS
Testowanie złożoności haseł i hashy za pomocą narzędzi hashcat oraz John the ripper, uzyskiwanie słowników i budowanie własnych

B. Problematyka laboratoriów

Część 1 (semestr 4)
Konfiguracja maszyn wirtualnych potrzebnych do realizacji laboratorium.
Wybrane podatności w aplikacjach internetowych (np. SQLi, XSS, CSRF, BAC, ...) – sprawdzanie występowania podatności, przykładowe wykorzystanie podatności, realizacja zabezpieczeń na poziomie aplikacji internetowej i bazy danych.
Część 2 (semestr 5)
Zapoznanie się z narzędziami do rekonesansu oraz ich dobór zależnie od potrzeb.
Uzyskiwanie dostępu do linii komend systemu operacyjnego różnymi narzędziami na podstawie wcześniejszego rekonesansu.
Uzyskiwania dostępu do sieci wewnętrznej za firewall, tunelowanie połączeń, przekierowywanie portów.
Testowanie praktyczne złożoności haseł i algorytmów hashujących, pozyskiwanie słowników i ich modyfikacje.

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, ...)
Część 1 (semestr 4)		
EK_01	kolokwium	wykład
EK_02	kolokwium	laboratorium
EK_03	obserwacja w trakcie zajęć	laboratorium
Część 2 (semestr 5)		
EK_04	kolokwium	laboratorium
EK_05	kolokwium	laboratorium

4.2 Warunki zaliczenia przedmiotu (kryteria oceniania)

Semestr 4:

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.

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 jest oceniany na 'zal.'/'nzal.' na podstawie aktywności w trakcie zajęć.

Ocena końcowa z laboratorium jest wystawiana na postawie oceny za efekt EK_02, pod warunkiem, że efekt EK_03 został oceniony na 'zal'.

Semestr 5:

Zaliczenie z wykładu uzyskiwane jest na podstawie kolokwium.
Efekt EK_04 uznany jest za zaliczony, gdy student odpowie poprawnie na przynajmniej połowę przypisanych do niego pytań.

Efekt EK_05 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).

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

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	60
Inne z udziałem nauczyciela akademickiego (udział w konsultacjach, egzaminie)	2
Godziny niekontaktowe – praca własna studenta (przygotowanie do zajęć, egzaminu, napisanie referatu itp.)	45
SUMA GODZIN	107
SUMARYCZNA LICZBA PUNKTÓW ECTS	4

** 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:

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:

1) Himanshu Sharma, Harpreet Singh , „Hands On Red Team Tactics A practical guide to
2) mastering Red Team operations", 2018
3) David Kennedy et al., „Metasploit : the penetration tester's guide", 2011
4) https://owasp.org/www-community/attacks/Blind_SQL_Injection
5) https://sekurak.pl/czym-jest-sql-injection/
6) https://sekurak.pl/czym-jest-podatnosc-csrf-cross-site-request-forgery/
7) https://sekurak.pl/czym-jest-cors-cross-origin-resource-sharing-i-jak-wplywa-na-bezpieczenstwo/
8) https://sekurak.pl/hsts-czyli-http-strict-transport-security/
9) https://sekurak.pl/owasp-top-ten-2021-a04-insecure-design-przeglad-przypadkow/
10) https://sekurak.pl/jak-w-prosty-sposob-zwiekszyc-bezpieczenstwo-aplikacji-webowej/