

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Bezpieczeństwo aplikacji webowych**
 Nazwa w języku angielskim: **Security of web applications**
 Karta przedmiotu ważna od roku akademickiego: **2022/2023**
 Kierunek studiów: **Informatyka**
 Poziom studiów: **Studia I stopnia**
 Forma studiów: **Niestacjonarne**
 Profil: **Praktyczny**
 Specjalność: **Cyberbezpieczeństwo**
 Język wykładowy: **Polski**
 Jednostka prowadząca: **Wydział Nauk Społecznych i Technicznych**
 Prowadzący: **dr hab. inż. Bartłomiej Sulikowski**

OBCIĄŻENIE STUDENTA

	Wykład	Konwersatorium	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć dydaktycznych organizowanych przez Uczelnię	14		14		
Liczba godzin całkowitego nakładu pracy studenta	50		50		
Forma zaliczenia	Egzamin		Zaliczenie z oceną		
Liczba punktów ECTS	2		2		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

Wiedza i umiejętności z zakresu przedmiotów: Nowoczesne systemy informatyczne, Systemy operacyjne, Podstawy cyberbezpieczeństwa.

CELE PRZEDMIOTU

C1	Zdobycie wiedzy i umiejętności związanych z zagrożeniami aplikacji webowych oraz procedurami monitorowania bezpieczeństwa i skutecznego reagowania na ataki.
C2	Zdobycie wiedzy i umiejętności związanych z projektowaniem i wdrażaniem mechanizmów zapewniających bezpieczeństwo w aplikacjach webowych.
C3	Ugruntowanie świadomości, że zapewnianie bezpieczeństwa systemów to proces ciągły, a nie jednorazowa procedura.

PRZEDMIOTOWE EFEKTY UCZENIA – PEU	
Z zakresu wiedzy:	
PEU_W01	Posiada wiedzę z zakresu identyfikowania zagrożeń aplikacji webowych oraz stosowania procedur i narzędzi służących do ich wykrywania zgodnie z dokumentami normatywnymi ISO/IEC z serii 27000.
PEU_W02	Posiada wiedzę na temat przeciwdziałania atakom na aplikacje webowe oraz wdrażania mechanizmów zabezpieczeń.
Z zakresu umiejętności:	
PEU_U01	Potrafi przeprowadzić praktyczną analizę mechanizmów aplikacji webowych pod kątem ich podatności na różne typy ataków.
PEU_U02	Potrafi zaprojektować i zaimplementować zabezpieczenia aplikacji webowych, minimalizujące ryzyko powstawania podatności na różne typy ataków.
Z zakresu kompetencji społecznych:	
PEU_K01	Jest gotów do współpracy z innymi osobami w organizacji oraz pracownikami podmiotów zewnętrznych, np. ISP, zarówno z podczas procedur monitorowania, wdrażania zabezpieczeń oraz reagowania na ataki w stosunku do aplikacji webowych. Zna zakres kompetencji pracowników pionu ochrony (w tym zespołów administratorów systemu informatycznego oraz zespołu inspektora bezpieczeństwa) w jednostce organizacyjnej w zakresie zabezpieczeń aplikacji webowych.

TREŚCI PROGRAMOWE		
Forma zajęć – wykład		Liczba godzin
W1	Wprowadzenie, omówienie zasad zaliczenia przedmiotu. Podstawy bezpieczeństwa oraz źródła zagrożeń aplikacji internetowych.	2
W2	Bezpieczeństwo systemów udostępniających dane przez Internet.	2
W3	Analiza ryzyka zgodnie z normą ISO/IEC 27005.	2
W4	Analiza działania i skuteczności mechanizmów zabezpieczeń zgodnie z metodologią OWASP i normą ISO/IEC 27001.	2
W5	Zasada minimalnych przywilejów użytkowników systemów webowych i bazodanowych.	2
W6	Protokoły i algorytmy kryptograficzne stosowane w procesie zapewniania bezpieczeństwa danych.	2
W7	Ataki SQL Injection i metody obrony.	2
Razem		14

Forma zajęć – laboratorium		Liczba godzin
L1	Wprowadzenie, omówienie zasad zaliczenia przedmiotu. PHP Injection i Webshell.	3
P2	XML RPC Code.	2

L3	XSS (Cross-Site Scripting).	2
L4	Zagrożenia złośliwym oprogramowaniem propagowanym poprzez usługę www.	2
L5	Wykrywanie zagrożeń i ich analiza zgodna z metodologią OWASP na bazie projektu VWAD.	3
L6	DDoS. Podsumowanie, zaliczenie.	2
Razem		14

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
1.	Prezentacja treści z wykorzystaniem multimediów.
2	Dyskusja dydaktyczna.
3	Praca własna/grupowa w laboratorium – przeprowadzenie analizy podatności aplikacji VWAD z wykorzystaniem Kali Linux i pakietów: NMap, Nikto, OWASP Zed Attack Proxy, SQLMap.
4	Praca własna/grupowa w laboratorium – ugruntowanie wiedzy i umiejętności z zakresu zastosowań protokołów i algorytmów kryptograficznych, pakiet programowy Cryptool.

METODY I FORMY OCENY

OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Formy oceny (F lub P)*	Numer efektu uczenia (przedmiotowego)	Metody oceny osiągnięcia efektu uczenia
F w	PEU_W01, PEU_W02, PEU_K01	Aktywność na zajęciach, Dyskusja moderowana przez prowadzącego.
P w	PEU_W01, PEU_W02, PEU_K01	Egzamin w formie pisemnej.
F I	PEU_U01, PU02, PEU_K01	Realizacja zestawu ćwiczeń grupowych.
P I	PEU_U01, PU02, PEU_K01	Średnia z ocen cząstkowych wystawianych indywidualnie po wykonaniu każdego ćwiczenia.

*F – ocena formująca (w trakcie semestru), P – ocena podsumowująca (na koniec semestru)

KRYTERIA OCENY

OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Nr PEU	Ocena dostateczna	Ocena dobra	Ocena bardzo dobra
PEU_W01	Wie jak zidentyfikować najczęściej spotykane zagrożenia aplikacji webowych.	Wie jak zidentyfikować zagrożenia aplikacji webowych oraz scharakteryzować procedury i narzędzia służące do ich wykrywania.	Posiada zaawansowaną wiedzę z zakresu identyfikowania zagrożeń aplikacji webowych oraz stosowania procedur i narzędzi służących do ich wykrywania.

PEU_W02	Wie jak scharakteryzować procedury i narzędzia stosowane podczas wdrażania mechanizmów zabezpieczeń aplikacji webowych.	Posiada wiedzę na temat przeciwdziałania atakom na aplikacje webowe oraz wdrażania mechanizmów zabezpieczeń.	Posiada zaawansowaną wiedzę na temat przeciwdziałania atakom na aplikacje webowe. Umie opisać i scharakteryzować procedury wdrażania i monitorowania mechanizmów zabezpieczeń, jak również przeciwdziałania skutkom ataków.
PEU_U01	Potrafi scharakteryzować podatności aplikacji webowych na różne typy ataków.	Potrafi przeprowadzić praktyczną analizę mechanizmów aplikacji webowych pod kątem ich podatności na najbardziej rozpowszechnione typy ataków.	Potrafi przeprowadzić praktyczną analizę mechanizmów aplikacji webowych pod kątem ich podatności na wszystkie typy ataków oraz, w przypadku niejednoznacznych rezultatów, przeprowadzić analizę z wykorzystaniem metod wnioskowania heurystycznego.
PEU_U02	Potrafi zaprojektować i zaimplementować podstawowe zabezpieczenia aplikacji webowych.	Potrafi zaprojektować i zaimplementować zabezpieczenia aplikacji webowych, minimalizujące ryzyka powstawania podatności na różne typy ataków.	Potrafi zaprojektować i zaimplementować zabezpieczenia aplikacji webowych, minimalizujące ryzyka powstawania podatności na różne typy ataków oraz przeprowadzić proces ewaluacji ich skuteczności.
PEU_K01	Rozumie konieczność współpracy z innymi osobami w organizacji oraz pracownikami podmiotów zewnętrznych, np. ISP, zarówno z podczas procedur monitorowania, wdrażania zabezpieczeń oraz reagowania na ataki w stosunku do aplikacji webowych.	Rozumie konieczność współpracy z innymi osobami w organizacji oraz pracownikami podmiotów zewnętrznych, np. ISP, zarówno z podczas procedur monitorowania, wdrażania zabezpieczeń oraz reagowania na ataki w stosunku do aplikacji webowych. Zdaje sobie sprawę z zakresu kompetencji pracowników pionu ochrony (w tym zespołów administratorów systemu informatycznego oraz zespołu inspektora bezpieczeństwa) w jednostce organizacyjnej w zakresie zabezpieczeń aplikacji webowych.	Rozumie konieczność współpracy z innymi osobami w organizacji oraz pracownikami podmiotów zewnętrznych, np. ISP, zarówno z podczas procedur monitorowania, wdrażania zabezpieczeń oraz reagowania na ataki w stosunku do aplikacji webowych. Zna zakres kompetencji pracowników pionu ochrony (w tym zespołów administratorów systemu informatycznego oraz zespołu inspektora bezpieczeństwa) w jednostce organizacyjnej w zakresie zabezpieczeń aplikacji webowych.

LITERATURA PODSTAWOWA

A. Hoffmann, Bezpieczeństwo nowoczesnych aplikacji internetowych. Przewodnik po zabezpieczeniach, wyd. O'Reilly, 2020.
Pr. zbior., Bezpieczeństwo aplikacji webowych, wyd. Sekuritem, 2022.

LITERATURA UZUPEŁNIAJĄCA

R. Messier, Kali Linux. Testy bezpieczeństwa, testy penetracyjne i etyczne hakowanie, wyd. Helion, 2019.
P. Hope, B. Walther, Testowanie bezpieczeństwa aplikacji internetowych. Receptury, wyd. Helion, 2010.
P. Prasad, Testy penetracyjne nowoczesnych serwisów. Kompendium inżynierów bezpieczeństwa, wyd. Helion, 2017.

MACIERZ POWIĄZANIA

EFEKTÓW UCZENIA DLA PRZEDMIOTU BEZPIECZEŃSTWO APLIKACJI WEBOWYCH

Z EFEKTAMI UCZENIA NA KIERUNKU INFORMATYKA

Przedmiotowy efekt uczenia	Odniesienie przedmiotowego efektu do efektów uczenia zdefiniowanych dla kierunku studiów i specjalności	Cele przedmiotu	Treści programowe	Numer narzędzia dydaktycznego
PEU_W01	K_W02, K_W03	C1, C3	W1, W2, W3, W4, P5, P6	1, 2, 3
PEU_W02	K_W05, K_W08	C2, C3	W3, W4, W5, W6, W7, P5	1,2, 3
PEU_U01	K_U02	C1, C3	P1-P6	3,4
PEU_U02	K_U07	C2, C3	P1-P6	3,4
PEU_K01	K_K01, K_K04	C3	P5	3