KARTA KURSU

Nazwa	**Bezpieczeństwo aplikacji internetowych**
Nazwa w j. ang.	Web Application Security

Koordynator	mgr Alfred Budziak	Zespół dydaktyczny
		mgr Alfred Budziak mgr Piotr Pyciński
Punktacja ECTS*	st. stacjonarne: 2 st. niestacjonarne: 2	

Opis kursu (cele kształcenia)

Celem kursu jest zapoznanie studentów z:
- zagrożeniami bezpieczeństwa aplikacji internetowych,
- popularnymi metodami ataków na aplikacje webowe
- metodami i urządzeniami do zabezpieczania aplikacji

Kurs prowadzony jest w języku polskim.

Warunki wstępne

Wiedza	Działanie i funkcjonowanie sieci z szczególnym naciskiem na protokół HTTP
Umiejętności	Programowanie w jednym z popularnych języków do tworzenia aplikacji webowych, PHP, RoR, Python Django
Kursy	Aplikacje Internetowe, Zaawansowane technologie sieciowe

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	Po zakończeniu kursu student: W01: Zna podstawowe zagrożenia bezpieczeństwa aplikacji webowych OWASP TOP 10, oraz popularne błędy programistów aplikacji internetowych	K_W03,K_W08,K_W13,
	W02: Wie jak zidentyfikować i zabezpieczyć system internetowy przed popularnymi atakami	K_W03,K_W08,K_W13

Umiejętności	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
	Po zakończeniu kursu student: U01: Potrafi przeskanować i przetestować podatności w aplikacji	K_U03,K_U04, K_U05
	U02: Potrafi wdrożyć i skonfigurować mechanizmy zabezpieczania aplikacji webowych	K_U05,K_U06

Kompetencje społeczne	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
	Po zakończeniu kursu student: K01: Potrafi zaprojektować elementy bezpieczeństwa w systemach informatycznych	K_K02, K_K04,K_K05

Studia stacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A	K	L	S	P	Z				
Liczba godzin	15			15							

Studia niestacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A	K	L	S	P	Z				
Liczba godzin	10			10							

Opis metod prowadzenia zajęć

Kurs składa się z wykładu i ćwiczeń prowadzonych w formie laboratoriów. W ramach wykładu zostaną studentowi przedstawiona podstawowa ogólna wiedza z zakresu bezpieczeństwa systemów komputerowych poszerzona o popularne zagrożenia bezpieczeństwa aplikacji webowych, sposoby myślenia osób atakujących, schematy ataków, popularne błędy programistów, metody obrony, dostępne na rynku urządzenia i zasady projektowania bezpieczeństwa. Na laboratorium studenci w środowisku kontrolowanym będą wykorzystywali wiedzę z wykładu do identyfikowania zagrożeń, wykrycia luk bezpieczeństwa, wdrożenia mechanizmów obrony w oparciu o narzędzia open source dostępne na rynku. Przedstawią też projekt wdrożenia zabezpieczeń w wybranym przez prowadzącego środowisku

Formy sprawdzania efektów uczenia się

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Zadania problemowe
W01								X					
W02					X			X					
U01					X			X					X
U02					X		X	X					X
K01					X		X	X					X

Kryteria oceny	Przygotowanie i przedstawienie projektu wdrożenia zabezpieczeń w wybranym przez prowadzącego środowisku, wykorzystującego wiedzę z wykładu i laboratoriów w szerokim zakresie jest warunkiem niezbędnym zaliczenia przedmiotu. Ocenę dobrą lub bardzo dobrą może uzyskać student, który w tworzonym projekcie wykorzysta bardziej zaawansowane rozwiązania.

Uwagi	

Treści merytoryczne (wykaz tematów)

1. SQLi,
2. XSS,
3. CSRF,
4. Session Hijacking,
5. Insecure Direct Object References,
6. Sensitive Data Exposure,
7. ModSecurity,
8. WEB Application Firewall,
9. Techniki ataków typu DoS i DDoS

Wykaz literatury podstawowej

1. A. Barczak, T. Sydoruk, Bezpieczeństwo systemów informatycznych, Wyd. Akademii Podlaskiej, 2002
2. R. Anderson, Inżynieria zabezpieczeń, Wyd. WNT, Warszawa 2005
3. M. D. Bauer, Linux : serwery, bezpieczeństwo, Wyd. Helion, Gliwice 2005
4. G, Anonim, Linux : agresja i ochrona, Wyd. robomatic, Wrocław 2000
5. P.Hope, Testowanie bezpieczeństwa aplikacji internetowych , Helion 2012

Wykaz literatury uzupełniającej

1. http://owasp.org/index.php/Main_Page
2. T. J. Klevinsky, Hack I.T. : testy bezpieczeństwa danych , Helion 2003
3. Eric Foster, Skrypty powłoki od podstaw Helion 2006
4. D.Chell – bezpieczeństwo aplikacji mobilnych , Helion 2018

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – **studia stacjonarne**

Liczba godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	5
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	5
	Realizacja zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu	5
	Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna lub w grupie)	5
	Przygotowanie do egzaminu/zaliczenia	
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – **studia niestacjonarne**

Liczba godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	10
	Pozostałe godziny kontaktu studenta z prowadzącym	2
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	5
	Realizacja zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu	15
	Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna lub w grupie)	8
	Przygotowanie do egzaminu/zaliczenia	
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2