

KARTA KURSU

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

Koordinator	Mgr inż. Kamil Migacz	Zespół dydaktyczny
		mgr inż. Kamil Migacz, dr inż. Rafał Szklarczyk
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 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, np. PHP, Ruby, Python, Java, C#
Kursy	<u>Wymagane zaliczenie kursu:</u> <ul style="list-style-type: none"> • Aplikacje Internetowe (Web Applications) • Zaawansowane technologie webowe

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

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	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 i zasady projektowania bezpieczeństwa.

Na laboratorium studenci w grupach przygotowują w oparciu o wybraną przez siebie technologię aplikację internetową demonstrującą podatności z grupy OWASP TOP10. Projekt będzie również posiadał wdrożenie zabezpieczeń przed zaimplementowanymi podatnościami.

W trakcie zajęć studenci będą wykorzystywać wiedzę z wykładu do identyfikacji zagrożeń, wykrycia luk bezpieczeństwa, wdrożenia mechanizmów obrony w oparciu o narzędzia open source dostępne na rynku.

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	<p>Przygotowanie i przedstawienie projektu wdrożenia zabezpieczeń, wykorzystującego wiedzę z wykładu i laboratoriów w szerokim zakresie jest warunkiem niezbędnym zaliczenia przedmiotu.</p> <p>Osiągnięcie efektów kształcenia podanych powyżej uprawnia studentów do uzyskania oceny nie wyższej niż dostateczna. Ocenę dobrą lub bardzo dobrą może uzyskać student, który:</p> <p>- umiejętności na ocenę 4 Potrafi poprawnie zidentyfikować oraz zabezpieczyć aplikację internetową oraz w jasny i zrozumiały sposób wyjaśnić metody ataku i obrony.</p> <p>- umiejętności na ocenę 5 Zna mechanizmy i narzędzia minimalizujące ryzyko wystąpienia podatności oraz potrafi je zademonstrować ich działanie + umiejętności na ocenę 4.</p>
----------------	--

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. Bezpieczeństwo aplikacji internetowych dla programistów. Rzeczywiste zagrożenia, praktyczna ochrona, M. McDonald, Helion 2021.
2. Podręcznik pentestera. Bezpieczeństwo systemów informatycznych, P. Kim, Helion 2015.
3. Testowanie bezpieczeństwa aplikacji internetowych, P.Hope, Helion 2012.

Wykaz literatury uzupełniającej

1. Kali Linux i testy penetracyjne. Biblia, G. Khawaja, Helion 2022.
2. Dokumentacja OWASP.
3. bezpieczeństwo aplikacji mobilnych, D.Chell, Helion 2018

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

Liczba godzin w kontakcie z prowadzącymi	Wykład	20
	Konwersatorium (ćwiczenia, laboratorium itd.)	30
	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	5
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3

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

Liczba godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	20
	Pozostałe godziny kontaktu studenta z prowadzącym	10
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	10
	Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna lub w grupie)	10
	Przygotowanie do egzaminu/zaliczenia	5
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3