



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Projekt współfinansowany przez
Unię Europejską w ramach
Europejskiego Funduszu
Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Nazwa przedmiotu		Kod ECTS					
Bezpieczeństwo aplikacji webowych		11.3.2000					
Nazwa jednostki prowadzącej przedmiot							
Instytut Informatyki							
Studia							
wydział	kierunek	poziom	pierwszego stopnia				
Wydział Matematyki, Fizyki i Informatyki	Informatyka	forma	stacjonarne				
		moduł	wszystkie				
		specjalnościowy	wszystkie				
		specjalizacja	wszystkie				
Nazwisko osoby prowadzącej (osób prowadzących)							
prof. UG, dr Jakub Neumann; mgr Konrad Sołtys							
Formy zajęć, sposób ich realizacji i przypisana im liczba godzin		Liczba punktów ECTS					
Formy zajęć		2					
Wykład, Ćw. laboratoryjne		Udział w zajęciach dydaktycznych, objętych planem studiów: 30h					
Sposób realizacji zajęć		Praca własna studenta: 20h					
zajęcia w sali dydaktycznej		RAZEM: 50h					
Liczba godzin							
Wykład: 15 godz., Ćw. laboratoryjne: 15 godz.							
Termin realizacji przedmiotu							
2024/2025 letni							
Status przedmiotu		Język wykładowy					
obowiązkowy		polski					
Metody dydaktyczne		Forma i sposób zaliczenia oraz podstawowe kryteria oceny lub wymagania egzaminacyjne					
<ul style="list-style-type: none"> - Dyskusja - Projektowanie doświadczeń - Wykład problemowy - ćwiczenia laboratoryjne -- sporządzanie i uruchamianie programów komputerowych 		Sposób zaliczenia					
		Zaliczenie na ocenę					
		Formy zaliczenia					
		<ul style="list-style-type: none"> - wykonanie pracy zaliczeniowej - projekt lub prezentacja - ustalenie oceny zaliczeniowej na podstawie ocen cząstkowych otrzymywanych w trakcie trwania semestru 					
		Podstawowe kryteria oceny					
		próg zaliczeniowy	składowa ocena końcowej				
projekt		60%	100%				
Sposób weryfikacji założonych efektów uczenia się							
zakładany efekt kształcenia	egzamin	kolokwium	projekt	referat	raport	aktywność	obserwacja postawy i umiejętności
	Wiedza						
K_W07			X				
	Umiejętności						
K_U03							X
K_U06							X
	Kompetencje						
K_K02							X

<p>Określenie przedmiotów wprowadzających wraz z wymogami wstępnymi</p> <p>A. Wymagania formalne Brak wymagań formalnych</p> <p>B. Wymagania wstępne Brak wymagań wstępnych</p>	
<p>Cele kształcenia</p> <p>Celem przedmiotu jest zapoznanie słuchaczy z zagadnieniami związanymi z bezpieczeństwem aplikacji internetowych w tym sposobów prawidłowego projektowania aplikacji pod kątem bezpieczeństwa, wykorzystania dedykowanych/specjalistycznych protokołów oraz przeciwdziałania popularnym atakom.</p>	
<p>Treści programowe</p> <ol style="list-style-type: none"> 1. Wprowadzenie do zagadnień bezpieczeństwa aplikacji webowych 2. Popularne rodzaje ataków na aplikacje webowe i mobilne 3. Protokoły OAuth2 i OpenId Connect 4. Zastosowanie i konfiguracja serwerów typu IAM (ang Identity and Access Management) 	
<p>Wykaz literatury</p> <p>A. Literatura wymagana do ostatecznego zaliczenia zajęć (zdania egzaminu):</p> <p>A.1. wykorzystywana podczas zajęć Dokumentacja/standardy: OAuth2: https://oauth.net/2/ OpenId Connect: https://openid.net/connect/</p> <p>A.2. studiowana samodzielnie przez studenta Aktualne blogi i artykuły tworzone przez specjalistów związane z aktualnie omawianą technologią Często występujące problemy i aktualne dyskusje związane z omawianymi technologiami: https://stackoverflow.com</p> <p>C. Literatura uzupełniająca Advanced API Security: Securing APIs with OAuth 2.0, OpenID Connect, JWS, and JWE, Prabath Siriwardena</p>	
<p>Kierunkowe efekty uczenia się</p> <p>K_W07 ma wiedzę w zakresie projektowania, wytwarzania, testowania, wdrażania i utrzymania aplikacji webowych oraz ich bezpieczeństwa</p> <p>K_U03 potrafi pracować w zespole informatyków, zarządzać swoim czasem oraz podejmować zobowiązania i dotrzymywać terminy, porozumiewać się przy użyciu różnych technik w środowisku zawodowym w tym z wykorzystaniem dedykowanych narzędzi</p> <p>K_U06 potrafi dbać o bezpieczeństwo danych, w tym o ich bezpieczne przesyłanie; posługuje się narzędziami szyfrowania danych</p> <p>K_K02 potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania</p>	<p>Wiedza</p> <p>zna różne protokoły związane z bezpieczeństwem aplikacji opartych na protokole HTTP, w szczególności protokół OAuth2 oraz OpenID Connect ma wiedzę w zakresie projektowania, wytwarzania, testowania, wdrażania i utrzymania aplikacji webowych oraz ich bezpieczeństwa</p>
	<p>Umiejętności</p> <p>potrafi zbudować aplikację klient - serwer z zabezpieczonym dostępem do API wg protokołu OAuth2/OpenID Connect umie skonfigurować wybrany serwer/usługę typu Identity Access Management potrafi pracować w zespole informatyków, zarządzać swoim czasem oraz podejmować zobowiązania i dotrzymywać terminy, porozumiewać się przy użyciu różnych technik w środowisku zawodowym w tym z wykorzystaniem dedykowanych narzędzi potrafi dbać o bezpieczeństwo danych, w tym o ich bezpieczne przesyłanie, posługuje się narzędziami szyfrowania danych</p>
	<p>Kompetencje społeczne (postawy)</p> <p>potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania</p>
<p>Kontakt</p> <p>jakub.neumann@ug.edu.pl</p>	