



**KAPITAŁ LUDZKI**  
NARODOWA STRATEGIA SPÓJNOŚCI

Projekt współfinansowany przez  
Unię Europejską w ramach  
Europejskiego Funduszu  
Społecznego

**UNIA EUROPEJSKA**  
EUROPEJSKI  
FUNDUSZ SPOŁECZNY



<b>Nazwa przedmiotu</b>		<b>Kod ECTS</b>					
Bezpieczeństwo aplikacji webowych		11.3.1068					
<b>Nazwa jednostki prowadzącej przedmiot</b>							
Instytut Informatyki							
<b>Studia</b>							
<b>wydział</b>	<b>kierunek</b>	<b>poziom</b>	<b>pierwszego stopnia</b>				
Wydział Matematyki, Fizyki i Informatyki	Informatyka	<b>forma</b>	stacjonarne				
		<b>moduł</b>	wszystkie				
		<b>specjalnościowy</b>	wszystkie				
		<b>specjalizacja</b>	wszystkie				
<b>Nazwisko osoby prowadzącej (osób prowadzących)</b>							
dr Wiesław Pawłowski; dr Andrzej Borzyszkowski							
<b>Formy zajęć, sposób ich realizacji i przypisana im liczba godzin</b>		<b>Liczba punktów ECTS</b>					
<b>Formy zajęć</b>		3					
Wykład, Ćw. laboratoryjne							
<b>Sposób realizacji zajęć</b>							
zajęcia w sali dydaktycznej							
<b>Liczba godzin</b>							
Ćw. laboratoryjne: 15 godz., Wykład: 15 godz.							
<b>Termin realizacji przedmiotu</b>							
2020/2021 letni							
<b>Status przedmiotu</b>		<b>Język wykładowy</b>					
obowiązkowy		polski					
<b>Metody dydaktyczne</b>		<b>Forma i sposób zaliczenia oraz podstawowe kryteria oceny lub wymagania egzaminacyjne</b>					
<ul style="list-style-type: none"> <li>- wykład problemowy</li> <li>- ćwiczenia audytorne - dyskusja</li> <li>- ćwiczenia laboratoryjne - projektowanie doświadczeń</li> <li>- ćwiczenia laboratoryjne -- sporządzanie i uruchamianie programów komputerowych</li> </ul>		<b>Sposób zaliczenia</b>					
		<ul style="list-style-type: none"> <li>- Zaliczenie na ocenę</li> <li>- Egzamin</li> </ul>					
		<b>Formy zaliczenia</b>					
		<ul style="list-style-type: none"> <li>- egzamin pisemny z pytaniami (zadaniami) otwartymi</li> <li>- egzamin pisemny testowy</li> <li>- ustalenie oceny zaliczeniowej na podstawie ocen cząstkowych otrzymywanych w trakcie trwania semestru</li> <li>- kolokwium</li> </ul>					
		<b>Podstawowe kryteria oceny</b>					
<b>Sposób weryfikacji założonych efektów kształcenia</b>							
zakładany efekt kształcenia	egzamin	kolokwium	projekt	referat	raport	aktywność	obserwacja postawy i umiejętności
	Wiedza						
K_W07	X	X					
	Umiejętności						
K_U03							X
K_U06							X
	Kompetencje						
K_K02							X

<b>Określenie przedmiotów wprowadzających wraz z wymogami wstępnymi</b>	
<b>A. Wymagania formalne</b> Brak wymagań formalnych	
<b>B. Wymagania wstępne</b> Brak wymagań wstępnych	
<b>Cele kształcenia</b> 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	
<b>Treści programowe</b> <ol style="list-style-type: none"> <li>1. Wprowadzenie do zagadnień bezpieczeństwa aplikacji webowych</li> <li>2. Popularne rodzaje ataków na aplikacje webowe i mobilne</li> <li>3. Protokół TLS/SSL, certyfikaty serwerów i klientów</li> <li>4. Protokoły OAuth2 i OpenId Connect</li> <li>5. Zastosowanie serwerów typu IAM (ang Identity and Access Management)</li> </ol>	
<b>Wykaz literatury</b> <p>A. Literatura wymagana do ostatecznego zaliczenia zajęć (zdania egzaminu):</p> <p>A.1. wykorzystywana podczas zajęć                  Dokumentacja/standardy:                  OAuth2: <a href="https://oauth.net/2/">https://oauth.net/2/</a>                  OpenId Connect: <a href="https://openid.net/connect/">https://openid.net/connect/</a>                  TLS: <a href="https://tools.ietf.org/html/rfc5246">https://tools.ietf.org/html/rfc5246</a></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:  <a href="https://stackoverflow.com">https://stackoverflow.com</a></p> <p>C. Literatura uzupełniająca                  Advanced API Security: Securing APIs with OAuth 2.0, OpenID Connect, JWS, and JWE, Prabath Siriwardena</p>	
<b>Kierunkowe efekty kształcenia</b>  P6S_WG K_W07 P6S_UW P6S_UK P6S_UU K_U03 K_U06 P6S_KK K_K02	<b>Wiedza</b>  ma wiedzę w zakresie projektowania, wytwarzania, testowania, wdrażania i utrzymania aplikacji webowych oraz ich bezpieczeństwa
	<b>Umiejętności</b>  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
	<b>Kompetencje społeczne (postawy)</b>  potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania
<b>Kontakt</b>  w.pawlowski@inf.ug.edu.pl	