University of Gdańsk

Subject card

Subject name and code	Safety od Web Applications, PG_00204172						
Field of study	Informatics						
Date of commencement of studies	October 2026		Academic year of realisation of subject	2027/2028			
Education level	Bachelor's studies		Subject group	Obligatory subject group in the field of study Subject group related to practical vocational preparation			
Mode of study	full-time studies		Mode of delivery	at the university			
Year of study	2		Language of instruction	Polish			
Semester of study	4		ECTS credits	2.0			
Learning profile	practical		Assessment form	credit			
Conducting unit	Institute of Informatics -> Faculty of Mathematics, Physics and Informatics -> Rector						
Name and surname of lecturer (lecturers)	Subject supervisor		dr Jakub Neumann				
	Teachers						
Lesson types	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	15.0	0.0	15.0	0.0	0.0	30
	E-learning hours included: 0.0						
Learning activity and number of study hours	Learning activity	Participation in didactic classes included in study plan		Participation in consultation hours		Self-study	SUM
	Number of study hours	30		0.0		20.0	50
Subject objectives	The aim of the course is to familiarize students with issues related to the security of web applications, including how to properly design applications in terms of security, the use of dedicated/specialized protocols and counteracting popular attacks. Particular emphasis is placed on OAuth2/OpenIDConnect protocols and the issue of secure API sharing						

Learning outcomes

Course outcome	Subject outcome	Method of verification
[INFPL3_K02] is ready to recognize the importance of knowledge in solving cognitive problems and practical and seeking opinions experts in case of difficulties with independent problem solving	can precisely formulate questions related to the security of web applications and OAuth2/ OpenIDConnect protocols, in particular use concepts such as Resource Server, Authorization Server, Resource Owner, Client, User Agent	[SK2] presentation/project/paper/ report [SK4] test/exam - oral or written
[INFPL3_W07] knows and understands facts and methods to an advanced degree in the field of designing, developing, testing, implementing and maintaining web applications and their security; applies this knowledge in practical projects, creating web applications and preparing their functional and performance tests	has knowledge related to web application security issues, counteracting popular attacks, in particular knows the rules related to flows/grants of the OAuth2/ OpenIDConnect protocols	[SW4] test/exam - oral or written [SW2] presentation/project/paper/ report
[INFPL3_U06] can take care of data security, including secure transmission; uses data compression and encryption tools	can safely serve APIs following the rules of OAuth2 flows/grants, use appropriate libraries to support OAuth2, manage the Keycloak authorization server	[SU2] presentation/project/paper/ report [SU4] test/exam - oral or written
[INFPL3_U03] is able to cooperate with other people within teamwork, including being able to manage his/her time, make commitments, communicate using various techniques in the professional environment, including the use of dedicated tools; is able to present different opinions and alternative technical solutions in the project team, explaining their basis, consequences and impact on the project implementation	is able to keep commitments, including time deadline, resulting from the implementation of project tasks, cooperate in a group carrying out similar projects/tasks	[SU2] presentation/project/paper/ report [SU4] test/exam - oral or written

Subject contents

- Authentication, authorization, IT system typical security issues
- HTTP protocol security, the role of the TLS protocol, securing the shared HTTP API
- HTTP Basic Authorization
- protocols OAuth2, Authorization Code Flow/Grant, Client Credential Flow/Grant, OpenID Connect
- configuration of authentication and authorization services on the example of the Auth0/Okta website
- local authentication and authorization service based on the example of the Keycloak server

Prerequisites and co-requisites

Passed course "Protokoły sieci web"

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
tests	51.0%	60.0%
projects	51.0%	40.0%

Recommended reading

Basic literature	Bezpieczeństwo nowoczesnych aplikacji internetowych. Przewodnik po zabezpieczeniach, aut. Andrew Hoffman, ISBN 9788328370050
Supplementary literature	Bezpieczeństwo aplikacji internetowych dla programistów. Rzeczywiste zagrożenia, praktyczna ochrona, aut.Malcolm McDonald, 9788328378032
eResources addresses	

Example issues/ example questions/ tasks being completed

Work placement

Not applicable

Document generated electronically. Does not require a seal or signature.