Module/Course Syllabus
Program: COMPUTER SCIENCE
Full-time master degree program

Course:	**Web Applications Security**
Type of the course:	elelctive
Course code:	I2S2.15
Year:	I
Semester:	II
Form of the degree program:	full-time
Form of classes and number of hours per semester:	60
Lecture	30
Classes	0
Laboratory	30
Project	0
Number of ECTS credits:	3
Form of assessment:	course completion assessment
Course language:	English

Course objective (CO)	
CO1	Familiarize students with the issues of Internet application security and solutions to increase their security.
CO2	Gain skills to detect vulnerabilities in Internet applications and create websites with a high degree of resistance to threats.

Prerequisites in terms of knowledge, skills and other competencies	
1	Knowledge of information security issues.
2	Internet application creating skills
3	Basic skills in the area of designing databases and SQL

Learning outcomes (LO)	
	In terms of knowledge:
LO 1	Student has the knowledge of web application security.
LO 2	Student has the knowledge necessary to select, design and implement mechanisms that increase the level of security of Internet applications.
	In terms of skills:
LO 3	A student has the skills to analyze the vulnerability of Internet applications against selected threats.
LO 4	A student is able to select, design, and implement security mechanisms in applications.
	In terms of social competence:
LO 5	A student is able to identify unethical behavior on the web and independently obeys netiquette.

Course content	
Form of classes – lectures (L)	
	Course content
L1	An introduction to web applications security.

L2	SQL injection attacks, defense mechanisms against SQLI.
L3	XSS attacks, defense mechanisms against XSS attacks.
L4	Authentication.
L5	Authorization.
L6	Users privileges in IT systems.
L7	Registering users activity in an IT system.
L8	Load balancing, reliability of communication between elements of an IT system.
L9	OWASP – an overview of reported threats.
Form of classes – laboratories (Lab)	
	Course content
Lab1	Laboratory work environment. Workstation configuration. Work rules.
Lab2	Security analysis of an IT system.
Lab3	Vulnerabilities search of an IT system or application.
Lab4	SQL injection, defense mechanisms implementation.
Lab5	XSS attacks, defense mechanisms implementation.
Lab6	Authentication.
Lab7	Users privileges in an IT system.
Lab8	Authorization.
Lab9	Users activity registering.

Didactic methods	
1	Conversational lecture.
2	Laboratory exercises: computer programming method.
3	Individual work

Assessment methods and criteria		
Assessment method symbol	**Assessment method description**	**Passing threshold**
A1	Laboratory: assessment of work done during laboratories	**51%**
A2	Written examination	**51%**

Required textbooks and other course materials	
1	OWASP Top 10 – 2021, https://owasp.org/www-project-top-ten/
2	Bezpieczeństwo aplikacji webowych, red. Michał Sajdak, Securitum 2021
Recommended textbooks and other course materials	
1	Bezpieczeństwo nowoczesnych aplikacji internetowych Przewodnik, Hoffmann Andrew, Helion 2020
2	A security analysis of authentication and authorization implemented in web applications based on the REST architecture, Tomasz Muszyński, Grzegorz Kozieł, JCSI - Journal of Computer Sciences Institute.- 2020, vol. 15, s. 252-260
3	Analiza możliwości obrony przed atakami SQL Injection, Chrystian Byzdra, Grzegorz Kozieł, JCSI - Journal of Computer Sciences Institute.- 2019, vol. 13, s. 339-344

Student workload	
Form of activity	**Average number of hours to complete the activity**
Contact hours with the lecturer, including:	60
participation in lectures	30

participation in laboratories	30
Student's own work, including:	15
preparation for the exam	5
preparation for the laboratory	10
Total student workload	75
Total number of ECTS credits	3

Learning outcomes matrix					
Learning outcome	**Reference to learning outcomes defined for the master's program**	**Course objectives**	**Course content**	**Didactic methods**	**Assessment methods**
LO 1	I2A_W08 ++	*CO1*	*L1-L9*	*1*	A2
LO 2	I2A_W07 +++	*CO1*	*L1-L9*	*1*	A2
LO 3	I2A_U01 ++	*CO2*	*Lab1-Lab9*	*2,3*	A1
LO 4	I2A_U10 +++	*CO2*	*Lab1-Lab9*	*2,3*	A1
LO 5	I2A_K01 +	*CO1,CO2*	*Lab1-Lab9, L1-L9*	*1,2,3*	A1, A2

The author of the program:	dr inż. Grzegorz Kozieł
E-mail address:	g.koziel@pollub.pl
Organizational unit:	Department of Computer Science