VIDZEMES AUGSTSKOLA

FACULTY OF ENGINEERING
STUDY COURSE DESCRIPTION

Course Title:	**Web application Penetration Testing**				
Course code (LAIS):	**MKI_021**				
Study programme:	**CYBERSECURITY ENGINEERING**				
Level of Study programme:	☐ 1st level professional higher education				
	☐ Professional Bachelor				
	☒ Professional Master				
	☐ PhD level				
Type of Study programme:	☐ Compulsory course (Part A)				
	☒ Professional specialization courses (Part B, compulsory)				
	☐ Professional specialization optional courses (Part B, optional)				
	☐ Elective courses (Part C)				
Course Workload:	**Credits**	**ECTS**	**Academic hours**	**Contact hours**	**Independent work hours**
	2	3	80	24	56
Course Author/ Tutor:	**Rūdolfs Gulbis**				
	Academic position scien./acad.degree	guest lecturer, Dr.ing.			
	Consultation: according to the schedule for each semester				
Course Form:	Full time				
Study year, semester:	2019./2020	3.sem.			
Language:	Latvian, English				
Prerequisites for the Course:	Basic skills in research, information search and processing				
Course Summary:	The aim of the course is to provide in-depth knowledge of standards, best practice in security testing specifically for web applications.				
Course Methods:	Lectures, practical workshops, discussions, group work				
The Type of Final examination	Exam				
Requirements for Credits:	Practical work 60%, final exam 40%				

Course Contents:	Introduction in Security Tests, Security Testing Standards, Techniques, Life Cycle, Web Architecture, Technologies, Detection and Use of Vulnerabilities	
Learning Outcomes	**Learning Outcomes**	**The evaluation methods and criteria**
	Knowledge	
	Student knows, understands and recognizes information security risks, vulnerabilities	lectures, practical classes, seminars, discussions, group work
	Skills	
	The student is able to apply appropriate methods to control and strengthen the information resources security	lectures, practical classes, seminars, discussions, group work
	Competency	
	Student is able to analyze, evaluate information security incidents, reduce its consequences and probability	practical classes, seminars, discussions, group work
Course Compulsory literature:	Anderson, R.J. 2008. Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Ed. New York, NY, USA: John Wiley & Sons. Accessed October 24, 2014 at http://www.cl.cam.ac.uk/~rja14/book.html	
Course additional literature:	RTFM: Read team manual, 2014 https://doc.lagout.org/rtfm-red-team-field-manual.pdf	
Course approval date:	2021-02-23	
Course last revision date:		

Study Course Plan:

Date*	Theme	Academic hours		Study Form
		contact lessons	**Independent work hours**	
	Introduction in Security Tests, Security Testing Standards, Techniques, Life Cycle,	8		Lecture, situation analysis, discussions
	Web Architecture, Technologies, Detection and Use of Vulnerabilities	8		Lecture, situation analysis, discussions
	Penetration testing tools for web app	6	20	Lecture, situation analysis, discussions, practical tasks
	Vulnerability assessment exercises		36	Course project development and presentation
	Group project	2		Open book exam
	Hours total:	***24***	***56***	

** The date is specified before the implementation of the course*