



COURSE UNIT DESCRIPTION

Course unit title	Course unit code
Website Security Testing (II Part)	ITWSTIIP

Lecturer	Department where the course unit is delivered
Coordinator: Teaching Assistant Virgilijus Krinickij	Department of Computational and Data Modeling Faculty of Mathematics and Informatics Vilnius University

Cycle	Type of the course unit
First	Individual

Mode of delivery	Semester or period when the course unit is delivered	Language of instruction
Face-to-face	Autumn	Lithuanian and English

Prerequisites
General understanding of UNIX operating systems, programming, and IT basics. Passed courses: Website Security Testing (I Part).

Number of ECTS credits allocated	Student's workload	Contact hours	Individual work
5	121	48	73

Purpose of the course unit: programme competences to be developed

Generic competences to be developed

- Ability to apply knowledge in practical situations (*BK1*)
- Ability for abstract thinking, processing and analysing information (*BK3*)
- Ability to resolve problems (*BK4*)

Subject-specific competences to be developed

- Ability to do program and IT service testing and debugging (*DK4*)
- Ability to validate the specification during project implementation (*DK3-2*)
- Ability to ensure information security using management and security mechanisms of operating systems and software (*DK8*)

Learning outcomes of the course unit	Teaching and learning methods	Assessment methods
Describe and identify potential risks of cyber-attacks to internet applications. Ability to assess possible attack difficulty and attack vector.	Cooperative lecture, situation analysis, project tasks, consulting.	Written exam, project task assessment.
Vulnerability analysis. Applying best practices for securing specific attack vectors.	Cooperative lecture, situation analysis, project tasks, consulting.	Written exam, project task assessment.
Ability to assess existing critical and non-critical infrastructure components, existing security solutions, and implement potential improvements.	Cooperative lecture, situation analysis, project tasks, consulting.	Written exam, project task assessment.
Agentic AI solution adaptability.	Cooperative lecture, situation analysis, project tasks, consulting.	Written exam, project task assessment.

Course content: breakdown of the topics	Contact hours							Individual work: time and assignments	
	Lectures	Consulting during lectures	Seminars	Tutorials	Laboratory work (LW)	Consulting during LW	Contact hours	Individual work	Assignments
1 Introduction, scope.	2				4		6	2	Preparation of laboratory environment.
2. Penetration Testing Execution Standard (PTES), OWASP WSTG.	2				4		6	5	WordPress and other presented websites preparation for audit.

3. Secure application architecture for penetration testers (2FA, TLS, authn/authz).	2				4		6	7	Website penetration testing using predefined tools.
4. Protection against XSS, CSRF, XXE and other attacks.	2				4		6	7	Website protection against other attack types.
5. Protection against malware injections, DoS and dependency risks, vulnerability management.	2				4		6	7	Website protection against other attack types and vulnerability management.
6. Agent-based artificial intelligence for penetration testing.	2				4		6	10	Agent usage for website penetration testing.
7. Workflow automation (n8n, MCP, LLMs).	2				4		6	10	Agent usage for system hardening.
8. Real attack channels, artificial intelligence-assisted attack chains, generated malicious code, automated scanning.	2				4		6	15	Agent usage for assisted attack chains.
Exam preparation								10	Consulting, material reading

Total:	16				32		48	73	
---------------	-----------	--	--	--	-----------	--	-----------	-----------	--

Assessment strategy	Weight %	Deadline	Assessment criteria
Exam	70%	At the end of the course	The number of correct answers to the questions asked.
Project work	30%	During the semester	Ability to apply security and general IT technologies, methodologies, tools, in different cases. The exam is allowed to be taken if 1.5 out of 3 points are collected in the project part.

Author	Publishing year	Title	Issue No or volume	Publishing house or Internet site
Required reading				
Orhan Yildirim	2026	Agentic AI for Offensive Cyber Security	Nr .1	Packt
Andrew Hoffman	2024	Web Application Security 2nd Edition	Nr. 2	O'Reilly Media



DALYKO APRAŠAS

Dalyko pavadinimas	Kodas
Svetainių saugumo testavimas (II dalis)	ITSSTIID

Dėstytojas	Padalinys
Koordinuojantis: Jaunesnysis Asistentas Virgilijus Krinickij	Kompiuterinio ir duomenų modeliavimo katedra Matematikos ir informatikos fakultetas Vilniaus universitetas

Studijų pakopa	Dalyko tipas
Pirmoji	Individualus

Igyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalbos
Auditorinė	Pavasario	Lietuvių ir anglų

Reikalavimai studijuojančiajam
Bendras UNIX operacinių sistemų, programavimo ir IT pagrindų išmanymas. Išklausyti kursai: Svetainių saugumo testavimas (I dalis).

Dalyko apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	121	48	73

Dalyko tikslas: studijų programos ugdomos kompetencijos
Bendrosios kompetencijos: - žinias taikyti praktikoje (BK1), - abstrakčiai mąstyti, analizuoti ir sisteminti informaciją (BK3), - spręsti problemas (BK4). Dalykinės kompetencijos: - testuoti, derinti programas ir IT paslaugas (DK4),

- patvirtinti specifikaciją projekto įgyvendinimo metu. (DK3-2) - užtikrinti informacijos saugumą panaudojant operacinių sistemų ir programinės įrangos valdymo bei apsaugos mechanizmus (DK8).		
Dalyko studijų siekiniai	Studijų metodai	Vertinimo metodai
Gebėjimas apibūdinti ir nustatyti, galimų kibernetinių atakų internetinėms aplikacijoms rizikas. Gebėjimas įvertinti galimos atakos sunkumą ir atakos vektorius.	Įtraukiamoji paskaita, situacijų analizė, projektinė veikla, konsultavimas.	Egzamino testas, projektinių užduočių atlikimas.
Gebėjimas pritaikyti geriausias praktikas saugumui užtikrinti.	Įtraukiamoji paskaita, situacijų analizė, gerų praktikų studija, projektinė veikla, konsultavimas.	Egzamino testas, projektinių užduočių atlikimas.
Gebėjimas įvertinti esamos kritinės ir nekritinės infrastruktūros komponentus, jau esamus įdiegtus saugumo sprendimus ir įdiegti galimus patobulinimus.	Įtraukiamoji paskaita, situacijų analizė, gerų praktikų studija, projektinė veikla, konsultavimas.	Egzamino testas, projektinių užduočių atlikimas.
Agentinio dirbtinio intelekto sprendimo pritaikomumas.	Įtraukiamoji paskaita, situacijų analizė, gerų praktikų studija, projektinė veikla, konsultavimas.	Egzamino testas, projektinių užduočių atlikimas.

Temos	Kontaktinio darbo valandos							Savarankiškų studijų laikas ir užduotys	
	Paskaitos (P)	Konsultacijos (P)	Seminariai	Pratybos	Laboratoriniai darbai	Konsultacijos (LD,)	Visas kontaktinis darbas	Savarankiškas darbas	Užduotys
1. Įvadas, apimtis.	2				2		4	2	Laboratorinės aplinkos pasiruošimas.
2. Įsilaužimo testavimo vykdymo standartas (angl. PTES), OWASP WSTG.	2				2		4	5	„Wordpress“ ir kitų pateiktų svetainių paruošimas auditui.
3. Saugi programų architektūra įsilaužimo testuotojams (2FA, TLS, authn/authz).	2				2		4	7	Svetainių įsilaužimo testavimas naudojant iš anksto nustatytus įrankius.
4. Apsauga nuo XSS, CSRF ir XXE ir kitų atakų.	2				2		4	7	Svetainių apsauga nuo kitų tipų atakų.
5. Apsauga nuo kenkėjiškų injekcijų, DoS ir priklausomybės rizikos, pažeidžiamumų valdymas.	2				2		4	7	Svetainių apsauga nuo kitų tipų atakų ir pažeidžiamumų valdymas.
6. Agentinis dirbtinis intelektas įsilaužimo testavimui.	2				2		4	10	Agentų naudojimas svetainių įsilaužimams testuoti.

7. Darbo eigos automatizavimas (n8n, MCP, LLMs).	2				2		4	10	Agentų naudojimas svetainių apsaugai.
8. Tikri puolimo kanalai, dirbtinio intelekto padedamos atakų grandinės, sugeneruotas kenkėjiškas kodas, automatizuotas skenavimas.	2				2		4	15	Agentų panaudojimas automatizuotam svetainių skenavimui ir kenkėjiško kodo aptikimui.
Pasiruošimas egzaminui ir jo laikymas								10	
Iš viso	16				32		48	73	

Vertinimo strategija	Svoris proc.	Atsiskaitymo laikas	Vertinimo kriterijai
Projektinis darbas	30%	Pratybų metu	Gebėjimas pritaikyti saugumo ir bendras IT technologijas, metodikas, įrankius, skirtingais atvejais. Egzaminą leidžiama laikyti, jei iš projektinės dalies yra surinkta 1.5 iš 3 balų.
Egzaminas	70%	Semestro pabaigoje	Teisingų atsakymų kiekis į pateiktus klausimus.

Autorius	Leidimo metai	Pavadinimas	Periodinio leidinio Nr. ar leidinio tomas	Leidimo vieta ir leidykla ar internetinė nuoroda
Privalomoji literatūra				
Orhan Yildirim	2026	Agentic AI for Offensive Cyber Security	Nr .1	Packt
Andrew Hoffman	2024	Web Application Security 2nd Edition	Nr. 2	O'Reilly Media