UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Varnost spletnih in mobilnih aplikacij
Course title:	Security of web and mobile applications

Študijski program in stopnja Study programme and level	Študijska smer Study field	Letnik Academic year	Semester Semester
Kibernetska varnost, magistrski študijski program druge stopnje	-	Drugi	Četrti
The second cycle master's study programme Cyber Security	-	Second	Fourth

Vrsta predmeta / Course type	Obvezni / Obligatory
Univerzitetna koda predmeta / University course code:	5-KV-MAG-VSMA-2021-12-14

Predavanja Lectures	Seminar Seminar	Vaje Tutorial	Klinične vaje work	Druge oblike študija	Samost. delo Individ. work	ECTS
30	/	30	/	/	120	6

Nosilec predmeta / Lecturer:	doc. dr. Pavle Boškoski

Jeziki / Languages:	**Predavanja / Lectures:**	Slovenski / Slovenian, Angleški / English
	Vaje / Tutorial:	Slovenski / Slovenian, Angleški / English

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisits:**
Za vključitev v delo je potrebno usvojiti vsebine predmeta Razvoj varne programske opreme.	In order to be included in work, it is necessary to master the content of the course Secure Software Development.

Vsebina:	**Content (Syllabus outline):**
Vsebina predmeta zagotavlja pregled varnostnih načel za razvoj spletne in mobilne aplikacije. Študenti bodo spoznali najbolj tipične strategije kibernetskih napadov in ustrezne obrambne pristope. To je zelo pomembno, saj se morajo danes razvijalci in oblikovalci zavedati varnostnih vprašanj na vsaki točki razvojnega cikla. Teme tega predmeta so razdeljene v dve glavni skupini:	The content of the exam provides an overview of security principles for development of web and mobile applications. The students will gain understanding of the most typical cyber-attack strategies and corresponding defense approaches. This is quite important since nowadays developers and designers must be aware of the security issues at every point of the development cycle.

1. Osnove in najsodobnejša spletna varnost. Teme vključujejo:

- načela spletne varnosti,
- napadi in protiukrepi,
- varnostni model brskalnika,
- ranljivosti spletnih aplikacij,
- vbrizgavanje kode,
- zavrnitev storitve,
- napadi TLS,
- zasebnost,
- prstni odtisi,
- politika istega izvora,
- večdomensko izvajanje kode,
- preverjanje pristnosti,
- obramba v globino in
- tehnike za pisanje varne kode.

2. Poglobljen pregled varnostnih funkcij in omejitev mobilnega operacijskega sistema, osnov mobilnih omrežij in varnosti mobilnega omrežja.

The topics in this course are divided in two main groups:

1. Fundamentals and the state-of-the-art in web security. Topics include:
   - principles of web security,
   - attacks and countermeasures,
   - the browser security model,
   - web app vulnerabilities,
   - code-injection,
   - denial-of-service,
   - TLS attacks,
   - privacy,
   - fingerprinting,
   - same-origin policy,
   - cross-site scripting,
   - authentication,
   - defense-in-depth, and
   - techniques for writing secure code.

2. In-depth overview of the security features and limitations of mobile operating system, basics of mobile networks and mobile network security.

Temeljni literatura in viri / Readings:

- Web Application Security: Exploitation and Countermeasures for Modern Web Applications 1st Edition by Andrew Hoffman. 2020. ISBN-13: 978-1492053118
- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition by Dafydd Stuttard. 2011. ISBN-13: 978-1118026472
- Web Security for Developers: Real Threats, Practical Defense Illustrated Edition by Malcolm McDonald. 2020. ISBN-13: 978-1593279943
- Microservices Security in Action: Design secure network and API endpoint security for Microservices applications, with examples using Java, Kubernetes, and Istio 1st Edition by Prabath Siriwardena, Nuwan Dias. 2020. ISBN-13: 978-1617295959

Cilji in kompetence:

Učna enota prispeva k razvoju naslednjih splošnih in predmetno-specifičnih kompetenc:

Splošne kompetence:

- Sposobnost identifikacije kibernetskih varnostnih tveganj ter izdelave predlogov za ukrepanje in zaščito na osnovi identificiranih tveganj.
- Sposobnost uporabe različnih programskih rešitev za zagotavljanje, upravljanje, nadzorovanje in evalvacijo kibernetske varnosti.

Objectives and competences:

The instructional unit contributes to the development of the following general and subject-specific competences:

General competences:

- The ability to identify cyber security risks and make proposals for action and protection based on identified risks.
- The ability to use various software solutions to provide, manage, monitor and evaluate cyber security.
- The ability to find data and sources for the needs of cyber security management.

- Sposobnost iskanja podatkov in virov za potrebe upravljanja kibernetske varnosti.
- Sposobnost fleksibilne uporabe pridobljenega znanja o kibernetski varnosti v praksi.

Predmetno-specifične kompetence:
- usposobljenost za vključevanje osnovnih varnostnih ukrepov pri razvoju spletnih in mobilnih aplikacij
- poznavanje osnov infrastrukture ključev za enkripcijo
- obvladovanje postopkov zagotavljanja varnega in stabilnega delovanja spletnih/mobilnih aplikacij
- razumevanje ključnih konceptov komunikacijske varnosti
- znanje in sposobnost praktične uporabe šifrirnih algoritmov, strategij varnega shranjevanja podatkov
- poznavanje osnovnih načel in tehnik za krepitev varnosti aplikacij

- The ability of flexible usage of the acquired knowledge on cyber security in practice.

Subject-specific competences:
- competence to incorporate basic security measures in the development of web and mobile applications
- familiarity with the basics of encryption keys infrastructure
- mastering procedures of ensuring safe and stable functioning of web/mobile applications
- understanding of the key concepts of communication security
- knowledge and the ability of practical use of encryption algorithms, safe data storage strategies
- knowledge of basic principles and techniques for strengthening application security

Predvideni študijski rezultati:

Znanje in razumevanje:

Študent:
- razume najpogostejše grožnje in ranljivosti spletnih in mobilnih aplikacij
- pridobi operativno znanje o pripravi osnovnih obrambnih protiukrepov
- se zaveda odnosa načrtovanje-funkcija in je sposoben ustrezno oblikovati varne aplikacije

Intended learning outcomes:

Knowledge and understanding:

The student:
- understands the most common threats and vulnerabilities of web and mobile applications
- gains operative knowledge of preparing basic defence countermeasures
- is aware of the design-function relationship and able to design secure applications accordingly

Metode poučevanja in učenja:
- *predavanja* z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje problemov)
- *vaje*, na katerih bodo študent na konkretnih problemih ponovili, utrdili in dodatno osvetlili pojme in metode, spoznane na predavanjih
- *domače naloge*: s katerimi bodo študenti spodbujeni, da sproti študirajo snov, ki bo obravnavana na predavanjih in vajah
- *seminarska naloga* bo študente naučila

Learning and teaching methods:
- *lectures* with active student participation (explanation, discussion, questions, examples, problem solving)
- *lab work,* during which the students will use practical problems to repeat and strengthen the topics and methods presented at the lectures
- *home works* will stimulate the students to study concurrently with lectures and lab work
- *student project* will prepare the students

samostojnega reševanja praktičnih problemov z uporabo standardnih podatkovnih struktur in algoritmov	to autonomously solve practical problems with the use of standard data structures and algorithms

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Vrsta (izpit, ustni, tečaj, projekt):		Type (examination, oral, coursework, project):
• Pisni izpit	25	• Written exam
• Naloge	75	• Assignments

Reference nosilca / Lecturer's references:

- BOŠKOSKI, Pavle, PERNE, Matija, RAMEŠA, Martina, MILEVA BOSHKOSKA, Biljana. Variational Bayes survival analysis for unemployment modelling. Knowledge-based systems, ISSN 0950-7051. [Print ed.], 11 Oct. 2021, vol. 229, [article no.] 107335, str. 1-11, doi: 10.1016/j.knosys.2021.107335. [COBISS.SI-ID 71383555]
- P. Boškoski. Towards digital transformation : implementation experience. International Conference on Information Society and Information Technologies - ISIT 2017, Novo mesto: Faculty of Information Studies 2017
- B. Mileva-Boshkoska, M. Bohanec, P. Boškoski, Đ. Juričić. Copula-based decision support system for quality ranking in the manufacturing of electronically commutated motors. Journal of intelligent manufacturing, 26 (2), 281-293, 2015
- A. Debenjak, P. Boškoski, B. Musizza, M. Kern, A. Biček. Informacijska arhitektura za proizvodno analitiko. Ventil : revija za fluidno tehniko in avtomatizacijo, ISSN 1318-7279, 23 (4), 284-288, 2017
- DAMIJ, Nadja, BOŠKOSKI, Pavle, BOHANEC, Marko, MILEVA BOSHKOSKA, Biljana. Ranking of business process simulation software tools with DEX/QQ hierarchical decision model. PloS one, ISSN 1932-6203, 2016, vol. 11, no. 2, str. 1-16, doi: 10.1371/journal.pone.0148391. [COBISS.SI-ID 29294119]