FIŞA DISCIPLINEI

Aspecte calitative ale securității în testarea software

Anul universitar 2025-2026

1. Date despre program

1.1. Instituţia de învăţământ superior	**Universitatea Babeş-Bolyai**
1.2. Facultatea	**Facultatea de Matematică şi Informatică**
1.3. Departamentul	**Departamentul de Informatică**
1.4. Domeniul de studii	**Informatică**
1.5. Ciclul de studii	**Master**
1.6. Programul de studii / Calificarea	**Securitate cibernetică (în limba engleză)**
1.7. Forma de învăţământ	**Cu frecvenţă**

2. Date despre disciplină

2.1. Denumirea disciplinei	**Aspecte calitative ale securităţii în testarea software**					Codul disciplinei	**MME8195**
2.2. Titularul activităţilor de curs	**Lector dr. Maria-Camelia Chisăliţă-Creţu**						
2.3. Titularul activităţilor de seminar	**Lector dr. Maria-Camelia Chisăliţă-Creţu**						
2.4. Anul de studiu	**1**	2.5. Semestrul	**1**	2.6. Tipul de evaluare	**C**	2.7. Regimul disciplinei	**Obligatoriu**

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1. Număr de ore pe săptămână	**4**	din care: 3.2. curs	**2**	3.3. seminar/ laborator/proiect	**2**
3.4. Total ore din planul de învăţământ	**56**	din care: 3.5. curs	**28**	3.6 seminar/laborator/proiect	**28**
Distribuţia fondului de timp pentru studiul individual (SI) şi activităţi de autoinstruire (AI)					**ore**
Studiul după manual, suport de curs, bibliografie şi notiţe (AI)					10
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					20
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii şi eseuri					40
Tutoriat (consiliere profesională)					12
Examinări					8
Alte activităţi: *comunicare cu titularul disciplinei*					4
3.7. Total ore studiu individual (SI) şi activităţi de autoinstruire (AI)				**94**	
3.8. Total ore pe semestru				**150**	
3.9. Numărul de credite				**6**	

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	• Programare orientată obiect, Metode avansate de programare, Medii de proiectare şi programare, Programare Web, Verificarea şi validarea sistemelor soft
4.2. de competenţe	• Cunoaşterea mediilor de programare pentru dezvoltarea aplicaţiilor în limbaje orientate-obiect de nivel înalt precum Java, C#, Python

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	• Sală de curs cu videoproiector
5.2. de desfăşurare a seminarului/ laboratorului	• Staţii de lucru şi utilizarea mediilor de dezvoltarea aplicaţiilor în limbaje de nivel înalt

6.1. Competenţele specifice acumulate[1]

[1] Se poate opta pentru competenţe sau pentru rezultatele învăţării, respectiv pentru ambele. În cazul în care se alege o singură variantă, se va şterge tabelul aferent celeilalte opţiuni, iar opţiunea păstrată va fi numerotată cu 6.

Competențe profesionale/esențiale	• Cunoașterea și înțelegerea principalelor paradigme care țin de protecția datelor: confidențialitatea, integritatea și disponibilitatea datelor. • Cunoașterea tuturor aspectelor de securitate care pot impacta procesele și infrastructura IT&C a unei organizații. • Utilizarea nuanțată și pertinentă a criteriilor și metodelor de verificare, validare și evaluare a soluțiilor software pentru a asigura securitatea acestora. • Capacitate avansată de analiză, proiectare și construcție securizată a sistemelor informatice, folosind o gamă variată de platforme hardware și software, limbaje și medii de programare și instrumente de modelare, verificare și validare.
Competențe transversale	• Abilități de comunicare profesională: descrierea clară, concisă, verbală și în scris a rezultatelor profesionale. • Comportarea onorabilă, etică, respectarea deontologiei profesionale. • Aplicarea regulilor de muncă organizată și eficientă, responsabilitate și seriozitate față de munca depusă atât individual cât și în echipă. • Spirit de inițiativă, antreprenorial; operarea cu cunoștințe economice, învățarea continuă.

6.2. Rezultatele învățării

Cunoștințe	Studentul cunoaște mecanismele de bază ce definesc securitatea sistemului și a mediului software în care se execută o aplicație, cum ar fi: permisiunile de acces, politicile de securitate, interacțiunea cu mediul exterior. Studentul cunoaște cele mai populare tipuri de atacuri cibernetice care se pot desfășura în Internet și are cunoștințe despre modul de evitare a unor asemenea atacuri. Studentul cunoaște tehnici eficiente de studiere și evaluare a unui cod sursă din perspectiva securității și capacitatea de a identifica posibile vulnerabilități.
Aptitudini	Studentul este capabil să dezvolte sisteme software securizate. Studentul este capabil să utilizeze tehnicile de securitate în dezvoltarea sistemelor software. Studentul este capabil să coordoneze activități de management de proiect, folosindu-se de abilități de decizie, de gândire critică și inovativă, precum și de abilități digitale.
Responsabilități și autonomie	Studentul are capacitatea de a evalua caracteristicile de securitate ale unei aplicații software la nivelul codului sursă. Studentul are capacitatea de a dobândi abilitățile de a utiliza diverse instrumente în procesul de testare pentru identificarea vulnerabilităților software. Studentul are capacitatea de lucra independent pentru a dobândi cunoștințe despre cele mai grave tipuri de vulnerabilități în domeniu, precum și despre măsurile de prevenție a acestor vulnerabilități.

7. Obiectivele disciplinei (reieșind din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	• Înțelegerea și aprofundarea noțiunii de testare de securitate și în particular testarea securității din perspectivă ofensivă (testare de penetrare) și testarea securității din perspectivă defensivă (testare de apărare). • Crearea unui mediu de explorare, exersare și aprofundare testării de securitatea folosind diferite scenarii practice. • Prezentarea unei imagini reale asupra conceptelor de testare de securitatea folosite industria software și a avantajelor acestora.

7.2 Obiectivele specifice	• Oferirea posibilității de a investiga multiple tehnici de testare software aplicate asupra unei varietăți de aspecte de securitate care fac referire la testarea de securitate ofensivă și testare de securitate defensivă. • Îmbunătățirea abilităților de testare focalizată de obiective. • Creșterea nivelului de înțelegere asupra tipurilor de vulnerabilități și a metodelor eficiente pentru identificarea acestora. • Utilizarea unor instrumente software actuale în procesul de testare de securitate. • Îmbunătățirea abilităților de proiectare a cazurilor de testare pornind de la obiective de testare stabilite, folosind tehnici de testare specifice pentru a investiga anumite vulnerabilități ale produsului soft dezvoltat.

8. Conținuturi

8.1 Curs	Metode de predare	Observații
Curs 1. Noțiuni introductive în testare - Testare software. Definiție, obiective, aplicabilitate - Tehnica de testare software. Definiție, atribute - Clasificarea tehnicilor de testare	Prezentare, Demonstrație, Problematizare	
Curs 2. Noțiuni introductive în securitatea software - Terminologie. Vulnerabilități - Tipuri de atacuri - Principii și standarde de lucru	Prezentare, Demonstrație, Problematizare	
Curs 3. Tehnici de testare bazate pe acoperire - Obiective. Aplicabilitate - Tours. Expresii logice - Testarea bazată pe specificații - Testarea bazată pe cerințe	Prezentare, Demonstrație, Problematizare	
Curs 4. Testare de securitate ofensivă - Definiție. Tipuri de vulnerabilități identificate - Abordări - Instrumente folosite	Prezentare, Demonstrație, Problematizare	
Curs 5. Tehnici de testare bazate pe risc (I) - Obiective. Aplicabilitate - HTSM - Liste de tipuri de erori	Prezentare, Demonstrație, Problematizare	
Curs 6. Tehnici de testare bazate pe risc (II) - Tehnica Quick-tests - Testarea bazata pe istoric - Testarea limitelor. Testarea de utilizabilitate	Prezentare, Demonstrație, Problematizare	
Curs 7. Tehnici de testare bazate pe activități - Obiective. Aplicabilitate - Tehnica Guerilla - Tehnica All-pairs - Testarea bazată de cazuri de utilizare - Testarea bazată pe scenarii de execuție	Prezentare, Demonstrație, Problematizare	
Curs 8. Testare de securitate defensivă - Definiție. Tipuri de vulnerabilități identificate - Abordări - Instrumente folosite	Prezentare, Demonstrație, Problematizare	
Curs 9. Tehnici de testare bazate pe evaluare - Obiective. Aplicabilitate - Testarea bazată echivalența	Prezentare, Demonstrație, Problematizare	

funcționalităților - Tehnica self-verifying data		
Curs 10. Tehnici de testare bazate pe rezultatul așteptat - Obiective. Aplicabilitate - Testarea de confirmare - Testarea de acceptanță	Prezentare, Demonstrație, Problematizare	
Curs 11. Analiza tehnicilor de testare bazate - Tehnici de testare bazate pe acoperire vs. Tehnici de testare bazate pe risc - Tehnici de testare bazate pe acoperire vs. Tehnici de testare bazate pe activități - Tehnici de testare bazate pe risc vs. Tehnici de testare bazate pe rezultatul așteptat - Tehnici de testare bazate pe rezultatul așteptat vs. Tehnici de testare bazate pe evaluare	Prezentare, Demonstrație, Problematizare	
Curs 12. Raportarea vulnerabilităților - Terminologie. Provocări legate de raportare - Strategia RIMGEA	Prezentare, Demonstrație, Problematizare	
Curs 13. Elaborarea proiectului de testare de securitate	Prezentare, Demonstrație, Problematizare	
Curs 14. Prezentarea proiectului de testare de securitate	Prezentare, Demonstrație, Problematizare	

Bibliografie

[Kaner99] C. Kaner, J. Falk, H.Q. Nguyen, Testing Computer Software, Wiley, 1999.
[Brn02] I. Burnstein, Practical Software Testing, Springer, 2002.
[Kaner02] C. Kaner, J. Bach, B. Pettichord, Lesson Learned in Software Testing, Wiley, 2002.
[Mye04] Glenford J. Myers, The Art of Software Testing, John Wiley & Sons, Inc., 2004.
[Nai08] K. Naik, P. Tripathy, Software testing and quality assurance. Theory and Practice, A John Wiley & Sons, Inc., 2008.
[Crs09] L. Crispin, J. Grecory, Agile testing: a practical guide for testers and agile teams, Addison-Wesley, 2009.
[Pres10] R. S. Pressman, Software engineering: a practinioner's approach, seventh edition, Higher Education, 2010.
[BBST2008] BBST – Bug Advocacy, http://www.testingeducation.org/BBST/bugadvocacy/BugAdvocacy2008.pdf
[BBST2010] BBST – Fundamentals of Testing, Cem Kaner, http://www.testingeducation.org/BBST/foundations/BBSTFoundationsNov2010.pdf.
[BBST2011] BBST – Test Design, Cem Kaner, http://www.testingeducation.org/BBST/testdesign/BBSTTestDesign2011pfinal.pdf
[Whitt2012] J. Whittaker, J. Arbon J. Carollo, How Google Tests Software, Google, Pearson Education, 2012.
[OWASP2014] QWASP, Testing guide 4.0, 2014, https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf
[NRVR2014] Ana Filipa Nogueira, José Carlos Ribeiro, Francisco Fernández de Vega, Mário Alberto Zenha-Rela, Object-Oriented Evolutionary Testing: A Review of Evolutionary Approaches to the Generation of Test Data for Object-Oriented Software, International Journal of Natural Computing Research 4(4):15-35, October, 2014.
[KMS2014] Kaur, Manpreet and Rupinder Singh. A Review of Software Testing Techniques, 2014.
[Meer2014] Joris Meerts, Functional Testing Heuritics, https://www.testingreferences.com/docs/Functional_Testing_Heuristics.pdf
[Draghia2019] Claudiu Draghia, Gamificarea in software testing. Testing Challenges, http://testingchallenges.thetestingmap.org/, 2019.
[ForK2019] István Forgács, Attila Kovács, Practical Test Design Selection of traditional and automated test design techniques, BCS, 2019.
[BSR2021] F. A. Bhuiyan, M. B. Sharif and A. Rahman, Security Bug Report Usage for Software Vulnerability Research: A Systematic Mapping Study, IEEE Access, vol. 9, pp. 28471-28495, 2021, doi: 10.1109/ACCESS.2021.3058067.
[AIW2021] Samah W.G. AbuSalim, Rosziati Ibrahim, Jahari Abdul Wahab, Comparative Analysis of Software Testing Techniques for Mobile Applications, Journal of Physics: Conference Series, vol 1793, 2021.
[PLGM2022] Sheena Panthaplackel, Junyi Jessy Li, Milos Gligoric, Raymond J. Mooney, Learning to Describe Solutions for Bug Reports Based on Developer Discussions, ACL 2022, pp. 2935 – 2952.
[CISA2024] Cybersecurity and Infrastructure Security Agency (CISA).
[IBM2024] International Business Machine (IBM), IBM Technologies.

[NIST2024] National Institute of Standards and Technology, Glossary.
[Abbas2017] Siddiqui, Abbas. (2017). Framework for Supervised & Secure Distributed Simulations of Critical Infrastructures.
[SentinelOne2024] SentinelOne, What Is A Threat Actor? – Types & Examples.
[Anand2022] Anand, P., Singh, Y., Singh, H. et al. SALT: transfer learning-based threat model for attack detection in smart home. Sci Rep 12, 12247 (2022). https://doi.org/10.1038/s41598-022-16261-9.
[Businesstech2021] Business Tech, Vulnerability Assessments: 4 Crucial Steps to Identify Vulnerabilities in Your Business.
[NCSC2016] NCSC, Common cyber attacks: reducing the impact.
[Baker2023] Kurt Baker, 10 Most Common Types of Cyber Attacks.
[Bergmans2023] Bart Lenaerts-Bergmans, 10 Types of social engineering attacks and how to prevent them.
[Zhuang] Rui Zhuang, Alexandru G. Bardas, Scott A. DeLoach, and Xinming Ou. 2015. A Theory of Cyber Attacks: A Step Towards Analyzing MTD Systems. In Proceedings of the Second ACM Workshop on Moving Target Defense (MTD '15). Association for Computing Machinery, New York, NY, USA, 11–20. https://doi.org/10.1145/2808475.2808478.
[MTechSystems2022] MTechSystems, The Most Common Cyber Attacks.
[Cyber2024] Cybersecurity Basics. NIST.
[Li2021] Yuchong Li, Qinghui Liu, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, 2021, Pages 8176-8186, ISSN 2352-4847, https://doi.org/10.1016/j.egyr.2021.08.126.

8.2 Seminar / laborator	Metode de predare	Observaţii
Seminar 1. Concepte de securitate. Cerinţele referatului pe teme de securitate	Prezentare, Conversaţie, Problematizare, Descoperire, Studiu individual, Exerciţiu	
Seminar 2. Securitatea aplicaţiilor	Prezentare, Conversaţie, Problematizare, Descoperire, Studiu individual, Exerciţiu	
Seminar 3. Vulnerabilităţi şi instrumente folosite în identificarea acestora	Prezentare, Conversaţie, Problematizare, Descoperire, Studiu individual, Exerciţiu	
Seminar 4. Prezentare referate	Prezentare, Conversaţie, Problematizare	
Seminar 5. Prezentare referate	Prezentare, Conversaţie, Problematizare	
Seminar 6. Prezentare referate	Prezentare, Conversaţie, Problematizare	
Seminar 7. Prezentarea proiectului de testare de securitate	Prezentare, Conversaţie, Problematizare	
Bibliografie *similară cu bibliografia de la curs*		

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

- Conţinutul disciplinei este în concordanţă cu recomandările ACM pentru domeniul informatică.
- Conţinutul cursului este inclus în programele de studii ale universităţilor de prestigiu din străinătate.
- Conţinutul cursului este considerat relevant de către companiile software care activează în domeniul asigurării securităţii software.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Proiectarea şi dezvoltarea unei soluţii de testare a unui produs software cu evidenţierea aspectelor de securitatea şi aplicarea tehnicilor de testare studiate. Nota proiectului este **P**.	Evaluare orală a proiectului	70%
10.5 Seminar/laborator	Referatul de la seminar va	Evaluarea orală a	30%

	fi notat. Nota referatului este **S**.	referatului	
Observații: • Proiectul de testare va fi realizat în echipe de 4-5 studenți. • Referatul de la seminar va fi realizat în echipe de 2-3 studenți.			
10.6 Standard minim de performanță			
• Studenții vor putea identifica vulnerabilități la testarea securității, într-o manieră similară cu derularea procesului de testare de securitate ofensivă și testare de securitate defensivă în industria software. • Studenții vor fi capabili să înțeleagă diferențele dintre tipurile de vulnerabilități, să identifice tipuri de atacuri și să elimine vulnerabilități. • Nota finală (M) se calculează astfel: M = 30%S+70%P. • Promovarea disciplinei presupune obținerea M>= 5.00.			

11. Etichete ODD (Obiective de Dezvoltare Durabilă / Sustainable Development Goals)[2]

Nu se aplică.

Data completării:	Semnătura titularului de curs	Semnătura titularului de seminar
15 aprilie 2025	**Lector dr. Maria-Camelia CHISĂLIȚĂ-CREȚU**	**Lector dr. Maria-Camelia CHISĂLIȚĂ-CREȚU**

Data avizării în departament:
...

Semnătura directorului de departament

Conf. dr. Adrian STERCA

[2] Păstrați doar etichetele care, în conformitate cu *Procedura de aplicare a etichetelor ODD în procesul academic*, se potrivesc disciplinei și ștergeți-le pe celelalte, inclusiv eticheta generală pentru *Dezvoltare durabilă* - dacă nu se aplică. Dacă nicio etichetă nu descrie disciplina, ștergeți-le pe toate și scrieți "*Nu se aplică.*".