

FIȘA DISCIPLINEI

(masterat)

1. Date despre program

Instituția de învățământ superior	Universitatea „Ștefan cel Mare” Suceava
Facultatea	Facultatea de Inginerie Electrică și Știința Calculatoarelor
Departamentul	Departamentul de Calculatoare, Electronică și Automatică
Domeniul de studii	Inginerie Electronică, Telecomunicații și Tehnologii Informaționale
Ciclul de studii	Master
Programul de studii	Securitate cibernetică

2. Date despre disciplină

Denumirea disciplinei	SECURITATEA APLICAȚIILOR WEB				
Titularul activităților de curs	prof.dr.ing. Corneliu TURCU				
Titularul activităților aplicative	ing. Eduard TIMOFTE				
Anul de studiu	II	Semestrul	1	Tipul de evaluare	E
Regimul disciplinei	Categorია formativă a disciplinei DSI – Discipline de sinteză; DAP – Discipline de aprofundare				DAP
	Categorია de opționalitate a disciplinei: DI - impusă, DO - opțională, DF - facultativă				DO

3. Timpul total estimat (ore alocate activităților didactice)

I a) Număr de ore, pe săptămână	3	Curs	1	Seminar		Laborator/lucrări practice	Laborator	2	Proiect	
I b) Totalul de ore (pe semestru) din planul de învățământ	42	Curs	14	Seminar		Laborator/lucrări practice	Laborator	28	Proiect	

II. Distribuția fondului de timp pe semestru	ore
II.a) Studiul după manual, suport de curs, bibliografie și notițe	45
II.b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren	20
II.b) Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	15
II.d) Tutoriat	0
III. Examinări	3
IV. Alte activități (precizați):	0

Total ore studiu individual II (a+b+c+d)	80
Total ore pe semestru (Ib+II+III+IV)	125
Numărul de credite	5

4. Precondiții (acolo unde este cazul)

Curriculum	• -
Competențe	• -

5. Condiții (acolo unde este cazul)

Desfășurare a cursului	• PC/laptop conectat la Internet, videoproiector și ecran, acces la Internet, note de curs, bibliografie recomandată.	
Desfășurare aplicații	Seminar	• -
	Laborator	• -
	Proiect	• PC/laptop conectat la Internet, videoproiector și ecran, acces la Internet, note de curs, bibliografie recomandată.

6. Competențe specifice acumulate

Competențe profesionale	<ul style="list-style-type: none"> • C1. Operarea cu fundamente tehnice și științifice în tehnologia informației și comunicațiilor, orientate cu precădere către aria Securității Cibernetică • C4. Însușirea tehnicilor de operare și utilizare a aparaturii și aplicațiilor profesionale specifice
-------------------------	--

	<p>ariei Securității Cibernetice</p> <ul style="list-style-type: none"> • C5. Identificarea și combaterea riscurilor și pericolelor privind expunerea sistemelor informatice la atacuri cibernetice • C6. Soluționarea incidentelor de securitate folosind instrumente specifice, proiectarea și dezvoltarea de instrumente și aplicații specifice securității cibernetice
Competențe transversale	<ul style="list-style-type: none"> • -

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

Obiectivul general al disciplinei	<ul style="list-style-type: none"> • Obiectivul acestei discipline îl constituie însușirea de către masteranzi a noțiunilor legate de securitatea aplicațiilor web. Se urmărește dezvoltarea experienței de proiectare și implementare a aplicațiilor web securizate, precum și de testare a securității acestora.
	<ul style="list-style-type: none"> • -

8. Conținuturi

Curs	Nr. ore	Metode de predare	Observații
1. Introducere în securitatea aplicațiilor web 1.1. Definiții și concepte de bază 1.2. Istoria și evoluția securității aplicațiilor web 1.3. Riscurile specifice aplicațiilor web	2	Expunerea, prelegerea, conversația, studii de caz, demonstrația.	
2. Amenințări și vulnerabilități ale aplicațiilor web	2		
3. Mecanisme de securitate pentru aplicațiile web	2		
4. Proiectarea, dezvoltarea și testarea aplicațiilor web în contextul asigurării securității 4.1. Utilizarea principiilor de securitate în proiectare 4.2. Implementarea mecanismelor de securitate în procesul de dezvoltare software 4.3. Testarea securității aplicațiilor web 4.4. Utilizarea inteligenței artificiale generative pentru asigurarea securității aplicațiilor web	4		
5. Gestionarea securității aplicațiilor web 5.1. Politici și proceduri de securitate 5.2. Educație și conștientizare 5.3. Monitorizare și răspuns la incidente	2		
6. Aspecte legale și etice ale securității aplicațiilor web 6.1. Legislația privind protecția datelor 6.2. Standarde de securitate 6.3. Proprietatea intelectuală 6.4. Confidențialitatea	2		

Bibliografie

- Ding, Ao, Gaolei Li, Xiaoyu Yi, Xi Lin, Jianhua Li, and Chaofeng Zhang. "Generative Artificial Intelligence for Software Security Analysis: Fundamentals, Applications, and Challenges." *IEEE Software*, 2024. <https://ieeexplore.ieee.org/abstract/document/10634314>
- Sai, Siva, Utkarsh Yashvardhan, Vinay Chamola, and Biplab Sikdar. "Generative Ai for Cyber Security: Analyzing the Potential of Chatgpt, Dall-e and Other Models for Enhancing the Security Space." IEEE Access, 2024. <https://ieeexplore.ieee.org/abstract/document/10491270>
- Sim K, Heo H, Cho H. Combating Web Tracking: Analyzing Web Tracking Technologies for User Privacy. *Future Internet*. 2024; 16(10):363. <https://doi.org/10.3390/fi16100363>
- Lu, Zhongyi, Declan T Delaney, and David Lillis. "A Survey on Microservices Trust Models for Open Systems." *IEEE Access* 11 (2023): 28840–55. <https://ieeexplore.ieee.org/abstract/document/10077578>
- Bhimireddy, Bhuvana Reddy, Alekhya Nimmagadda, Harshith Kurapati, Leelendra Reddy Gogula, Radhika Rani Chintala, and Vijaya Chandra Jadala. "Web Security and Web Application Security: Attacks and Prevention." In *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 1:2095–96. IEEE, 2023. <https://ieeexplore.ieee.org/document/10112741>
- S. Patil, M. Rao, L. Misal, D. Phaldesai and K. Shivsharan, "A Review of the OW ASP Top 10 Web Application Security Risks and Best Practices for Mitigating These Risks," *2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, Pune, India, 2023, pp. 1-8, doi: 10.1109/ICCUBEA58933.2023.10392030.
- A. Khanum, S. Qadir and S. Jehan, "OWASP-Based Assessment of Web Application Security," *2023 18th International Conference on Emerging Technologies (ICET)*, Peshawar, Pakistan, 2023, pp. 240-245, doi:

10.1109/ICET59753.2023.10374730.

- Pavel, Chudinov, and Babenko Ludmila. "Analysis of the Semantic Webs for Their Information Security." In *2023 16th International Conference on Security of Information and Networks (SIN)*, 1–4. IEEE, 2023. <https://ieeexplore.ieee.org/document/10475092>
- Indrianingsih, Yuliani, Aldin Gamas Pamungkas, Hero Wintolo, Haruno Sajati, Dwi Nugraheny, and others. "Descriptive Analysis of Web Security Vulnerabilities at Airport Servers Using The Open Web Application Security Project Security Standard." In *2023 International Conference on Electrical and Information Technology (IEIT)*, 6–11. IEEE, 2023. <https://ieeexplore.ieee.org/document/10335586>
- *, Web of Things (WoT) Architecture 1.1, 2023, <https://www.w3.org/TR/wot-architecture11/>
- Henriksen-Bulmer J, Yucl C, Faily S, Chalkias I. Privacy Goals for the Data Lifecycle. *Future Internet*. 2022; 14(11):315. <https://doi.org/10.3390/fi14110315>
- ZIAEV, Alexandr, Securitatea aplicațiilor web după modelul OWASP, Universitatea Tehnică a Moldovei, 2017
- Buraga, S., Securitatea aplicațiilor Web, Facultatea de Informatică, UAIC Iași, România, 2016: <http://www.slideshare.net/busaco/1313-web-securitatea-aplicatiilor-web>
- Articole științifice și de specialitate specifice

Aplicații (Seminar / laborator / lucrări practice / proiect)	Nr. ore	Metode de predare	Observații
1. Testarea pentru vulnerabilități tip file inclusion	2	Lucrări practice, studii de caz, evaluare.	
2. Analiza securității formularelor web și a validării input-ului	2		
3. Audit de securitate pentru funcția de upload de fișiere	2		
4. Testarea autentificării multifactor pentru o aplicație web	2		
5. Analiza actualizărilor și patch-urilor de securitate la nivel de aplicație web	2		
6. Auditul comunicării prin canale securizate (HTTPS, SSL, TLS)	2		
7. Identificarea vulnerabilităților tip information disclosure în aplicația web	2		
8. Testarea pentru brute force a credențialelor de autentificare web	2		
9. Analiza configurației de securitate a serverului de aplicație web	2		
10. Auditul jurnalelor aplicației web pentru anomalii de securitate	2		
11. Analiza mecanismelor de protecție împotriva atacurilor de forță brută	2		
12. Testarea funcționalității de logout pentru prevenirea sesiunilor neautorizate	2		
13. Auditarea implementării principiului least privilege în gestionarea accesului	2		
14. Evaluarea soluțiilor de securitate pentru interfețele de tip API	2		

Bibliografie

- R. Enriquez and A. Salazar C., RESTful java web services security. Birmingham, England: Packt Publishing, 2023.
- K. Beaver, Hacking for dummies, 7th ed. For Dummies, 2022.
- K. Crawley, 8 steps to better security: A simple cyber resilience guide for business. Nashville, TN: John Wiley & Sons, 2021.
- D. Clinton, Linux Security Fundamentals. Indianapolis, IN: Sybex, 2020.
- P. Siriwardena and N. Dias, Microservices security in action. New York, NY: Manning Publications, 2020.
- C. Panek, Security Fundamentals. Indianapolis, IN: Sybex, 2019.
- ZIAEV, Alexandr, Securitatea aplicațiilor web după modelul OWASP, Universitatea Tehnică a Moldovei, 2018
- Buraga, S., Securitatea aplicațiilor Web, Facultatea de Informatică, UAIC Iași, România, 2016: <http://www.slideshare.net/busaco/1313-web-securitatea-aplicatiilor-web>
- J. P. Mueller, Security for web developers: Using JavaScript, HTML, and CSS. O'Reilly Media, 2015.
- K. Kotwica, The benefits and security risks of web-based applications for business: Trend report. Philadelphia, PA: Elsevier Science Publishing, 2013.
- W. Stanek, Web applications, security & maintenance: The personal trainer for IIS 7.0 & IIS 7.5. Stanek & Associates, 2014.
- P. Engebretson, The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy.

Rockland, MA: Syngress Media, 2013.

- H. Islam, Security issues of web applications in Asp.net platform. LAP Lambert Academic Publishing, 2012.
- M. Harwood, Security strategies in web applications and social networking. Sudbury, MA: Jones and Bartlett, 2010.
- A. Chryssanthou, I. Apostolakis, and I. Varlamis, Eds., Certification and security in health-related web applications: Concepts and solutions. Hershey, PA: Medical Information Science Reference, 2010.
- S. Garfinkel and G. Spafford, Practical UNIX and Internet Security, 3rd ed. Sebastopol, CA: O'Reilly Media, 2003.
- B. Sullivan and V. Liu, Web application security, A beginner's guide. New York, NY: Osborne/McGraw-Hill, 2000.

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

- Conținutul cursului și al proiectului, prin problematica tratată, pune la dispoziția studentului cunoștințele necesare în domeniul tehnologiilor web. Tematica abordată se regăsește la universități de renume, dintre care se pot aminti: Universitatea Babeș-Bolyai - Facultatea de Matematică și Informatică, Universitatea „Alexandru Ioan Cuza” din Iași - Facultatea de Informatică, University of Lund (UK), Boston University (USA) etc..
- Compatibilitate națională:
 - Universitatea „Babeș-Bolyai” din Cluj-Napoca, Facultatea de Matematică și Informatică, disciplina „Securitate software”: https://www.cs.ubbcluj.ro/files/curricula/2020/syllabus/IE_sem5_MLR8114_ro_mihai-suciu_2020_5296.pdf;
 - Universitatea “Alexandru Ioan Cuza” Iași, Facultatea de Informatică, disciplinele “Modele de securitate”, “Protocoloale de Securitate: modelare și verificare”, <https://www.info.uaic.ro/wp-content/uploads/2022/10/MSI-ro.pdf>;
 - Universitatea “1 Decembrie 1918” din Alba Iulia, Facultatea de de Științe Exacte și Inginerești , disciplina “Securitatea Sistemelo Informatice” , https://www.uab.ro/media/documente/INFO_315_Securitatea_sitemelor_informatice.docx.pdf
- Compatibilitate internațională:
 - Lund University, Faculty of Engineering, „Web Security”, https://kurser.lth.se/kursplaner/22_23%20eng/EITF05.html
 - Centurion University, Penetration Testing & Vulnerability Assessment, <https://courseware.cutm.ac.in/courses/penetration-testing-vulnerability-assessment/>
 - Universidade de Aveiro, 42138 – „Technologies and Web Development”: <https://www.ua.pt/en/uc/15381> (2023)
 - Universitatea Tehnică a Moldovei, Securitatea aplicațiilor web după modelul OWASP, <http://repository.utm.md/handle/5014/13355>
 - Boston University, MET CS 701 – „Rich Internet Application Development”: <https://www.bu.edu/met/degrees-certificates/ms-computer-information-systems-web-application-development/#degree> (2023)

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Înșușirea cunoștințelor teoretice. Cunoașterea terminologiei utilizate în domeniu și capacitatea de comunicare folosind limbaj de specialitate.	Evaluarea prin test grilă a cunoștințelor din tematica studiată în timpul semestrului.	40%
Seminar	-	-	
Laborator	-	-	
Proiect	Demonstrarea capacității de analiză, sinteză, abstractizare și concretizare a cunoștințelor teoretice și practice, în construirea unor argumentări, în identificarea unor probleme și a soluțiilor acestora.	Evaluarea temelor de laborator.	60%
Standard minim de performanță			
Curs: <ul style="list-style-type: none">• capacitatea de a folosi un limbaj adecvat într-o discuție pe teme de specialitate;• capacitatea de analiză și sinteză a studiilor și lucrărilor științifice;• cunoașterea a cel puțin 50% din cantitatea de informație vehiculată la orele de instruire. Laborator: <ul style="list-style-type: none">• abilitatea de a înțelege și folosi termeni de specialitate în rezolvarea temelor de laborator;• capacitatea de a răspunde cerințelor temelor din lucrările de laborator.			

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicație
------------------	-------------------------------	------------------------------------

20.09.2023		
Data avizării	Semnătura responsabilului de program	
20.09.2023		
Data avizării în departament	Semnătura directorului de departament	
22.09.2023		
Data aprobării în consiliul facultății	Semnătura decanului	
27.09.2023		