FIŞA DISCIPLINEI

Anul universitar 2022-2023

Decan,
Prof. Vasile-Ion Manta

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică „Gheorghe Asachi” din Iași
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare și tehnologia informației
1.5 Ciclul de studii[1]	Master
1.6 Programul de studii	Securitatea spatiului cibernetic

2. Date despre disciplină

2.1 Denumirea disciplinei/Cod		Securitate web / SSC.IA.203					
2.2 Titularul activităților de curs		ș.l. dr. ing. Adrian Alexandrescu					
2.3 Titularul activităților de aplicații		ș.l. dr. ing. Adrian Alexandrescu					
2.4 Anul de studii[2]	2	2.5 Semestrul[3]	3	2.6 Tipul de evaluare[4]	examen	2.7 Tipul disciplinei[5]	DS

3. Timpul total estimat al activităților zilnice (ore pe semestru)

3.1 Număr de ore pe săptămână	4	din care 3.2 curs	2	3.3a sem.	-	3.3b laborator	1	3.3c proiect	1
3.4 Total ore din planul de învățământ[6]	56	din care 3.5 curs	28	3.6a sem.	-	3.6b laborator	14	3.6c proiect	14

Distribuția fondului de timp[7]	Nr. ore
Studiul după manual, suport de curs, bibliografie și notițe	24
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren	25
Pregătire seminarii/laboratoare/proiecte, teme, referate și portofolii	30
Tutoriat[8]	10
Examinări[9]	5
Alte activități:	

3.7 Total ore studiu individual[10]	94
3.8 Total ore pe semestru[11]	150
3.9 Numărul de credite	6

4. Precondiții (acolo unde este cazul)

4.1 de curriculum[12]	• -
4.2 de competențe	• -

5. Condiții (acolo unde este cazul)

5.1 de desfășurare a cursului[13]	• Sală de curs dotată cu videoproiector, tablă și acces internet
5.2 de desfășurare a seminarului / laboratorului / proiectului[14]	• Sală de laborator cu calculatoare și acces la internet • Sisteme de operare: Linux • Pachete software: diverse framework-uri web

6. Competențele specifice acumulate[15]

		Număr de credite alocat disciplinei[16]: **6**	Repartizare credite pe competențe[17]
Competențe profesionale	CP1	Cunoașterea conceptelor avansate din domeniul științei calculatoarelor și tehnologiei informației și capacitatea de a opera cu aceste concepte.	1.0
	CP2	Cercetarea științifică și practică privind securitatea sistemelor informatice complexe.	1.5
	CP3	Rezolvarea problemelor pe baza metodelor și tehnologiilor de securizare a sistemelor informatice complexe.	1.3
	CP4	Utilizarea de instrumente specifice domeniului în vederea identificării vulnerabilităților și a amenințărilor de securitate cibernetică.	1.0
	CP5	Proiectarea și dezvoltarea de soluții software cu un înalt grad de securitate orientate pe prevenția și răspunsul la incidente de securitate cibernetică.	0.7
	CP6		
	CPS1		
	CPS2		
Competențe transversale	CT1	Aplicarea, în contextul respectării legislației, a drepturilor de proprietate intelectuală, a principiilor, normelor și valorilor codului de etică profesională în cadrul propriei strategii de muncă riguroasă, eficientă și responsabilă.	0.1
	CT2	Identificarea rolurilor și responsabilităților într-o echipă specializată, luarea deciziilor și atribuirea de sarcini, cu aplicarea de tehnici de relaționare și muncă eficientă în cadrul	0.2

		echipei.	
	CT3	Dezvoltarea spiritului de creativitate, inițiativă și acțiune, pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională.	0.2
	CTS		

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

7.1 Obiectivul general al disciplinei	• Familiarizarea studenților cu modalitățile de securizare a aplicațiilor web.
7.2 Obiective specifice	• Cunoașterea tipurilor de vulnerabilități din perspectiva aplicațiilor web, • Cunoașterea modalităților de securizare a aplicațiilor web, • Cunoașterea modalităților de control a accesului, • Cunoașterea modalităților de detectare și protejare împotriva atacurilor web, • Abilități în identificarea posibilelor atacuri web.

8. Conținuturi

8.1 Curs[18]	Metode de predare[19]	Observații
1. Tehnologii web – concepte generale, arhitectura unei aplicații web (2h) 2. Protocolul HTTP. Cookie și sesiuni – posibile vulnerabilități (2h) 3. Protocolul HTTPS – certificate digitale și certificate digitale false ('man-in-the-middle', vulnerabilități PKI) (2h) 4. Serverele web și istoricul vulnerabilităților de securitate (2h) 5. Phishing, web scams, furt de identitate, scurgere de informații, spam (2h) 6. Deep și dark web, prezența utilizatorului pe forumuri, sandbox, honepot, whitelisting, blacklisting, reclame online (2h) 7. Securizarea formularelor, injecție de cod (SQLi, XSS), CORS, sanitizarea, obfuscarea codului, manipularea motoarelor de căutare (includere de link-uri sponsorizate cu referințe spre site-uri malițioase) (2h) 8. Analiza comportamentului utilizatorului. Monitorizarea și analiza traficului web. Compromiterea informațiilor confidențiale (încălcare a securității datelor) (2h) 9. Modalități de realizare a controlului accesului – protocoale de autentificare și autorizare (2h) 10. Securitatea framework-urilor web (2h) 11. Securitatea în e-commerce (2h) 12. Web Application Penetration Testing (2h) 13. Confidențialitatea și securitatea în Web 2.0 și Web 3.0 (2h) 14. AI și automatizare pentru gestionarea amenințărilor de securitate web (2h)	Cursul se predă folosind retroproiectorul și tabla și implică discuții cu studenții pe marginea subiectelor prezentate.	-
Bibliografie curs: 1. Stuttard, Dafydd, and Marcus Pinto. The web application hacker's handbook: Finding and exploiting security flaws. John Wiley & Sons, 2011. 2. Sullivan, Bryan, and Vincent Liu. Web application security, a beginner's guide. McGraw-Hill Education Group, 2011. 3. Baloch, Rafay. Ethical hacking and penetration testing guide. CRC Press, 2017. 4. Khawaja, Gus. Practical Web Penetration Testing: Secure web applications using Burp Suite, Nmap, Metasploit, and more. Packt. 2018 5. Zalewski, Michal. The tangled Web: A guide to securing modern web applications. No Starch Press, 2012. 6. Garfinkel, Simson, and Gene Spafford. Web security, privacy & commerce. " O'Reilly Media, Inc.", 2002.		
8.2a Seminar	Metode de predare[20]	Observații
-	-	-
8.2b Laborator	Metode de predare[21]	Observații
1. Analiza log-urilor unui server web în vederea detecției unor potențiale intruziuni. 2. Crearea unei soluții de tipul honeypot. 3. Realizarea unei aplicații de management al utilizatorilor cu accent pe acces sigur și pe detecția atacurilor (include whitelisting, blacklisting, controlul drepturilor utilizatorilor, protejarea împotriva man-in-the-middle). 4. Extinderea aplicației de management al utilizatorului prin integrarea unui protocol de autentificare. 5. Proiectarea și implementarea unei soluții de phishing. 6. Aplicarea tehnicilor de securizare într-o aplicație web care folosește un framework. 7. Căutarea și fructificarea vulnerabilităților unor site-uri prin injecție de cod.	Demonstrații, discuții, analiză și implementare aplicații.	-
8.2c Proiect	Metode de predare[22]	Observații
1. Prezentarea specificațiilor proiectului și formarea unor echipe 2. Alegerea temei de proiect și stabilirea, în linii mari, a tehnologiilor utilizate 3. Lucru la proiect	Demonstrații, discuții, analiză și implementare aplicații.	-

4. Prezentarea design-ului arhitecturii proiectului și a componentelor acestuia 5. Lucru la proiect 6. Lucru la proiect 7. Evaluarea proiectelor realizate		

Bibliografie aplicații (seminar / laborator / proiect):

1. Cursul de Securitate web
2. Sullivan, Bryan, and Vincent Liu. Web application security, a beginner's guide. McGraw-Hill Education Group, 2011
3. https://oauth.net/2/

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului[23]

- Cunoștințele acumulate în cadrul acestei discipline sunt necesare atât pentru o bună proiectare a aplicațiilor web cât și pentru abilitatea de a dezvolta componente software performante, scalabile și ușor de întreținut.
- Competențele dobândite vizează, în principal, familiarizarea studenților cu securizarea serviciilor și a aplicațiilor web.
- Domeniul web este unul extrem de dinamic, iar cererea pe piața muncii pentru specialiști în acest domeniu este în continuă creștere, deoarece tendința generală este ca aplicații din Internet să comunice prin intermediul serviciilor web.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare		10.3 Pondere din nota finală
10.4a Examen / Colocviu	• Cunoștințe teoretice și practice însușite (cantitatea, corectitudinea, acuratețea)	Teste pe parcurs[24]:	-	40% (minim 5)
		Teme de casă:	-	
		Alte activități[25]:	-	
		Evaluare finală: probă scrisă sau pe calculator, cu întrebări tip grilă și cu întrebări care necesită detalierea răspunsurilor.	100% (minim 5)	
10.4b Seminar	• Frecvența/relevanța intervențiilor sau răspunsurilor	Evidența intervențiilor, portofoliu de lucrări (referate, sinteze științifice)		-
10.4c Laborator	• Cunoașterea aparaturii, a modului de utilizare a instrumentelor specifice; evaluarea unor instrumente sau realizări, prelucrarea și interpretarea unor rezultate	• Răspuns oral • Demonstrație practică		20% (minim 5)
10.4d Proiect	• Calitatea proiectului realizat, corectitudinea documentației proiectului, justificarea soluțiilor alese	• Autoevaluarea, prezentarea și/sau susținerea proiectului • Evaluarea critică a unui proiect		40% (minim 5)
10.5 Standard minim de performanță[26] Familiarizarea cu fundamentele securității web. Cunoașterea aspectelor referitoare la tipurile de atacuri web și a modalităților de protejare împotriva acestora.				

Data completării, 13.01.2021

Semnătura titularului de curs, Ș.l.dr.ing. Adrian Alexandrescu

Semnătura titularului de aplicații, Ș.l.dr.ing. Adrian Alexandrescu

Data avizării în departament, 13.01.2021

Director departament, Conf.dr.ing. Andrei Stan

[1] *Licență / Master*
[2] *1-4 penrtru licență, 1-2 pentru master*
[3] *1-8 pentru licență, 1-3 pentru master*
[4] *Examen, colocviu sau VP A/R – din planul de învățământ*
[5] *DF - disciplină fundamentală, DID - disciplină în domeniu, DS – disciplină de specialitate sau DC - disciplină complementară - din planul de învățământ*
[6] *Este egal cu 14 săptămâni* x *numărul de ore de la punctul 3.1 (similar pentru 3.5, 3.6abc)*
[7] *Liniile de mai jos se referă la studiul individual; totalul se completeaza la punctul 3.7.*
[8] *Între 7 și 14 ore*

[9] *Între 2 și 6 ore*
[10] *Suma valorilor de pe liniile anterioare, care se referă la studiul individual.*
[11] *Suma dintre numărul de ore de activitate didactică directă (3.4) și numărul de ore de studiu individual (3.7); trebuie să fie egală cu numărul de credite alocat disciplinei (punctul 3.9)* x *24 de ore pe credit.*
[12] *Se menționează disciplinele obligatoriu a fi promovate anterior sau echivalente*
[13] *Tablă, vidoproiector, flipchart, materiale didactice specifice etc.*
[14] *Tehnică de calcul, pachete software, standuri experimentale, etc.*
[15] *Competențele din Grilele G1 și G1bis ale programului de studii, adaptate la specificul disciplinei, pentru care se repartizează credite (www.rncis.ro sau site-ul facultății)*
[16] *Din planul de învățământ*
[17] *Creditele alocate disciplinei se distribuie pe competențe profesionale și transversale în funcție de specificul disciplinei*
[18] *Titluri de capitole și paragrafe*
[19] *Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții (pentru fiecare capitol, dacă este cazul)*
[20] *Discuții, dezbateri, prezentare și/sau analiză de lucrări, rezolvare de exerciții și probleme*
[21] *Demonstrație practică, exercițiu, experiment*
[22] *Studiu de caz, demonstrație, exercițiu, analiza erorilor etc.*
[23] *Legătura cu alte discipline, utilitatea disciplinei pe piața muncii*
[24] *Se va preciza numărul de teste și săptămânile în care vor fi susținute.*
[25] *Cercuri științifice, concursuri profesionale etc.*
[26] *Se particularizează la specificul disciplinei standardul minim de performanță din grila de competențe a programului de studii, dacă este cazul.*