

FIȘA DISCIPLINEI

Noțiuni avansate de securitate software

Anul universitar 2025-2026

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Babeș-Bolyai
1.2. Facultatea	Matematică și Informatică
1.3. Departamentul	Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclu de studii	Master
1.6. Programul de studii / Calificarea	Securitate cibernetică
1.7. Forma de învățământ	Cu frecvență

2. Date despre disciplină

2.1. Denumirea disciplinei		Noțiuni avansate de securitate software				Codul disciplinei		MME8199
2.2. Titularul activităților de curs			Conf. univ. dr. ing. Mihai SUCIU					
2.3. Titularul activităților de seminar			Conf. univ. dr. ing. Mihai SUCIU					
2.4. Anul de studiu	2	2.5. Semestrul	3	2.6. Tipul de evaluare	E	2.7. Regimul disciplinei	Obligativu	

3. Timpul total estimat (ore pe semestru al activităților 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 învățământ	56	din care: 3.5. curs	28	3.6 seminar/laborator/proiect	28
Distribuția fondului de timp pentru studiul individual (SI) și activități de autoinstruire (AI)					ore
Studiul după manual, suport de curs, bibliografie și notițe (AI)					30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					20
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii și eseuri (mai mare sau egal cu nr. total ore prevăzut în calendarul disciplinei pentru temele de control)					35
Tutoriat (consiliere profesională)					4
Examinări					5
Alte activități [de ex.: comunicare bidirecțională cu titularul de disciplină / tutorele]					
3.7. Total ore studiu individual (SI) și activități de autoinstruire (AI)				94	
3.8. Total ore pe semestru				150	
3.9. Numărul de credite				6	

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	- Arhitectura sistemelor de calcul - Sisteme de operare - Structuri de date și algoritmi - Baze de date - Programare web
4.2. de competențe	Programare în C, cunoștințe de baza ale arhitecturii Intel x86, elemente de bază în programarea web și SQL.

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Sală dotată cu videoproiector
5.2. de desfășurare a seminarului/ laboratorului	Laborator cu calculatoare

6.1. Competențele specifice acumulate¹

Competențe profesionale/ esențiale	- Cunoașterea și înțelegerea principalelor paradigme care țin de protecția datelor: confidențialitatea, integritatea și disponibilitatea datelor. - Însușirea modului de funcționare a principalelor forme de aplicații malware și a principalelor forme de atacuri în Internet, precum și a metodelor de protecție împotriva acestora.
Competențe transversale	- Abilități de comunicare profesională: descrierea clară, concisă, verbală și în scris a rezultatelor profesionale. - Comportarea onorabilă, etică, respectarea deontologiei profesionale.

6.2. Rezultatele învățării

Cunoștințe	Studentul cunoaște cele mai bune mecanisme de securitate care pot fi implementate în Internet, dobândește cunoștințe despre cele mai grave tipuri de vulnerabilități în domeniu, precum și despre măsurile de prevenție a acestor vulnerabilități.
Aptitudini	Studentul este capabil să identifice posibilele probleme de securitate în sistemele software; are capacitatea de a evalua caracteristicile de securitate ale unei aplicații software la nivelul codului sursă.
Responsabilități și autonomie	Studentul are capacitatea de a lucra independent pentru a identifica vulnerabilitățile și amenințările de securitate la adresa unei organizații sau afaceri.

7. Obiectivele disciplinei (reieșind din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	- Capacitatea evaluării caracteristicilor de securitate ale unei aplicații software la nivelul codului sursă. - Dobândirea deprinderilor fundamentale minimale de scriere a unui cod sursă fără vulnerabilități.
7.2 Obiectivele specifice	- Cunoașterea mecanismelor de bază ce definesc securitatea sistemului și a mediului software în care se execută o aplicație (i.e. modelul de securitate), cum ar fi: permisiunile de acces, politicile de securitate, interacțiunea cu mediul exterior etc. - Cunoașterea principalelor tipuri de vulnerabilități software, precum: utilizarea datelor utilizator nevalidate corespunzător, interacțiunea necontrolată directă sau indirectă cu mediul exterior aplicației etc. - Deprinderea unor tehnici eficiente de studiere și evaluare a unui cod sursă din perspectiva securității și capacitatea de a identifica posibile vulnerabilități. - Capacitatea de a evalua implicațiile unei vulnerabilități descoperite. - Cunoașterea tehnicilor și a bibliotecilor de funcții utile în scrierea unui cod sursă fără vulnerabilități și capacitatea de a le utiliza în situații reale.

¹ Se poate opta pentru competențe sau pentru rezultatele învățării, respectiv pentru ambele. În cazul în care se alege o singură variantă, se va șterge tabelul aferent celeilalte opțiuni, iar opțiunea păstrată va fi numerotată cu 6.

8. Conținuturi

8.1 Curs	Metode de predare	Observații
Concepte și aspecte de bază referitoare la vulnerabilitățile software și la metodele și uneltele de dezvoltare a unui software fără vulnerabilități și de evaluare a unui software din perspectiva posibilelor vulnerabilități	Expunere la tablă, prezentare cu video proiectorul, discuții, probleme scurte	
Vulnerabilități de corupere a memoriei (buffer/integer overflow etc.)		
Vulnerabilități specifice limbajului C: limite aritmetice (de reprezentare), conversii de tip, pointeri etc.		
Vulnerabilități în componentele structurale ale unei aplicații software (Program building blocks)		
Vulnerabilități în utilizarea și manipularea șirurilor de caractere și meta caractere		
Vulnerabilități specifice sistemelor de operare UNIX		
Vulnerabilități de sincronizare (în situații de concurență)		
Vulnerabilități Web: injectare cod SQL, XSS, XSRF etc.		
Vulnerabilități de criptografie: parole vulnerabile, numere aleatoare previzibile etc.		
Metode de evaluare a (codului) unei aplicații din perspectiva securității: asigurarea calității, testare, gestiunea vulnerabilităților identificate		
Metode de evaluare a (codului) unei aplicații din perspectiva securității: asigurarea calității, testare, gestiunea vulnerabilităților identificate		
Metode de evaluare a (codului) unei aplicații din perspectiva securității: asigurarea calității, testare, gestiunea vulnerabilităților identificate		
Metode de evaluare a (codului) unei aplicații din perspectiva securității: asigurarea calității, testare, gestiunea vulnerabilităților identificate		
Metode de evaluare a (codului) unei aplicații din perspectiva securității: asigurarea calității, testare, gestiunea vulnerabilităților identificate		
Bibliografie		
8.2 Seminar / laborator	Metode de predare	Observații
Unelte utile în identificarea și evaluarea vulnerabilităților unui cod sursă: navigatoare prin codul sursă, depanatoare, navigatoare prin codul executabil (binar), testare fuzzy	Scurte expuneri la tablă,, ghiduri de lucru, demonstrații, explicații suplimentare, discuții, propunerea spre rezolvare a unor probleme de diferite tipuri și grade de complexitate.	
Tehnici de evitare, detecție și evaluare a vulnerabilităților de corupere a memoriei si specifice limbajului C		
Tehnici de evitare, detecție și evaluare a vulnerabilităților de utilizare și gestionare a șirurilor de caractere și meta caractere		
Tehnici de evitare, detecție și evaluare a vulnerabilităților specifice sistemului de operare Linux		
Tehnici de evitare, detecție și evaluare a vulnerabilităților aplicațiilor Web si aplicațiilor de retea		

Tehnici de evitare, detecție și evaluare a vulnerabilităților aplicațiilor Web și aplicațiilor de rețea		
Tehnici de evitare, detecție și evaluare a vulnerabilităților aplicațiilor Web și aplicațiilor de rețea		
Bibliografie 1. M. Down, J. McDonald, J. Schuh, „ The Art of Software Security Assessment. Identifying and Preventing Software Vulnerabilities ”, Addison-Wesley, 2007 2. M. Howard, D. LeBlanc, J. Viega, „ 24 Deadly Sins of Software Security. Programming Flows and How to Fix Them ”, McGraw Hill, 2010 3. M. Howard, D. LeBlanc, „ Writing Secure Code for Windows Vista ”, Microsoft Press, 2007 4. G. McGraw, „ Software Security: Building Security In ”, Addison-Wesley, 2006 5. R. Seacord, „CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems”, Addison-Wesley, 2 nd edition, 2014 6. 7, „ Common Weaknesses Enumeration (WCE)”, on-line: http://cwe.mitre.org/data/index.html		

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

Se realizează prin discuții periodice cu reprezentanți ai angajatorilor semnificativi din domeniul securității informației. Cursuri referitoare la aspecte de securitate în dezvoltarea aplicațiilor și domenii adiacente (de exemplu teste de penetrare) sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, la universități din țară și străinătate, cum ar fi: · Securitatea sistemelor software , Master de Securitatea informației, Universitatea Al. I. Cuza, Iași, Facultatea de calculatoare, http://profs.info.uaic.ro/~webdata/planuri/master/MISS1FS03.pdf · Securitatea sistemelor și aplicațiilor , Master de Securitatea tehnologiei informației, Academia Tehnică Militară, București, http://mta.ro/masterat/masterinfosec/curricula2013.html · Secure Software Systems , Master of Science in Information Security, Carnegie Mellon University, SUA, http://www.ini.cmu.edu/degrees/msis/courses.html · Software Security , Master in Information Security, Royal Holloway University of London, Information Security Group, https://www.royalholloway.ac.uk/isg/documents/pdf/coursespecs(msc)/modules201314/iy5607softwaresecurityspec1314.pdf
--

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Abilitatea de definire a conceptelor specifice problemelor de securitate la nivel de cod sursă și de expunere a metodelor de evaluare și dezvoltare corectă a unui cod sursă din perspectiva securității. · Abilitatea de rezolvare a unor probleme specifice domeniului.	Examen scris	60
10.5 Seminar/laborator	Abilitatea de rezolvare a unor probleme specifice domeniului · Prezență, (inter)activitate în timpul orelor de laborator/proiect.	Realizarea activităților de laborator și/sau rezolvarea temelor de casă și/sau a unor probleme în cadrul unui test practic	20%(activitate pe parcurs)+20%(test seminar)
10.6 Standard minim de performanță			

- Capacitatea de a defini vulnerabilitățile software fundamentale, precum: buffer overflow, injectare code SQL, XSS etc.
- Capacitatea de a identifica vulnerabilitățile software fundamentale și de a corecta codul (demonstrate în cadrul exercițiilor de laborator și a evaluării finale).
- Nota: minim 5 la fiecare activitate de notare.
- Prezențe: 75% prezență la activitățile de seminar.
- Studenții cu mai mult de 2 absențe nemotivate la seminar nu vor putea susține examenul în sesiunea normală și/sau în sesiunea de restanțe (activitățile de seminar sunt activități care se desfășoară pe principiul „activitate pe parcursul semestrului”, și nu pot fi recuperate sau repetate pentru o eventuală reluare a examenului (acești studenți vor trebui să repete acest curs în următorul an universitar)). Studenții cu certificate medicale pentru fiecare dintre absențe sunt exceptați de la această regulă.

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

Nu se aplică.

Data completării:
13.04.2025

Semnătura titularului de curs

Conf. Dr. Mihai SUCIU

Semnătura titularului de seminar

Conf. Dr. Mihai SUCIU

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*".