# FIŞA DISCIPLINEI

## 1. Date despre program

| | |
|---|---|
| 1.1 Instituţia de învăţământ superior | Universitatea Babeș-Bolyai |
| 1.2 Facultatea | Matematică și Informatică |
| 1.3 Departamentul | Departamentul de Informatică |
| 1.4 Domeniul de studii | Informatică |
| 1.5 Ciclul de studii | Licență |
| 1.6 Programul de studiu / Calificarea | Informatică |

## 2. Date despre disciplină

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2.1 Denumirea disciplinei | Securitate Software | | | | | | |
| 2.2 Titularul activităţilor de curs | Lect. Dr. Mihai SUCIU | | | | | | |
| 2.3 Titularul activităţilor de seminar | Drd. Raul TOȘA | | | | | | |
| 2.4 Anul de studiu | 3 | 2.5 Semestrul | 5 | 2.6. Tipul de evaluare | C | 2.7 Regimul disciplinei | Opțională |
| 2.8 Codul disciplinei | MLR8114 | | | | | | |

## 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 | 0+1+1 |
| 3.4 Total ore din planul de învăţământ | 56 | Din care: 3.5 curs | 28 | 3.6 seminar/laborator | 14 |
| Distribuţia fondului de timp: | | | | | ore |
| Studiul după manual, suport de curs, bibliografie şi notiţe | | | | | 28 |
| Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren | | | | | 28 |
| Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri | | | | | 38 |
| Tutoriat | | | | | 0 |
| Examinări | | | | | 2 |
| Alte activităţi: ..... | | | | | 0 |

| | |
|---|---|
| 3.7 Total ore studiu individual | 94 |
| 3.8 Total ore pe semestru | 150 |
| 3.9 Numărul de credite | 4 |

## 4. Precondiţii

| | |
|---|---|
| 4.1 de curriculum | • Arhitectura sistemelor de calcul<br>• Sisteme de operare<br>• Structuri de date și algoritmi<br>• Baze de date<br>• Programare web |
| 4.2 de competenţe | Programare in C, cunoștințe de baza ale arhitecturii Intel x86, elemente de bază în programarea web și SQL. |

**5. Condiţii**

| | |
|---|---|
| 5.1 De desfăşurare a cursului | • Sală dotată cu videoproiector |
| 5.2 De desfăşurare a seminarului/laboratorului | • Laborator cu calculatoare cu Visual Studio (C++) |

**6. Competenţele specifice acumulate**

| | |
|---|---|
| **Competenţe profesionale** | • C1.1 Cunoașterea noțiunilor, conceptelor și principiilor teoretice și practice aferente domeniului general al securității informațiilor. Identificarea și înțelegerea problemelor de securitate ce pot apărea în contextul unor limbaje specifice.<br>• C1.2 Evaluarea unor proiecte software existente și identificarea greșelilor de securitate din punctul de vedere al arhitecturii, modului de programare sau procedurilor de testare. Abilitatea de a efectua *code review* , cu scopul de a elimina erori ce afecteaza nivelul de securitate al aplicațiilor software.<br>• C1.4 Dezvoltarea unor module software sau a unor utilitare care să ajute la asigurarea unui înalt grad de securitate. Propunerea unor scenarii și modalități de testare a unor proiecte existente, cu scopul de a asigura / verifica calitatea lor din punctul de vedere al securității.<br>• C2.1 Cunoașterea principiilor și noțiunilor de bază necesare proiectării, dezvoltării și întreținerii unui cod sigur din punctul de vedere al securității ( *secure coding* ). Cunoașterea claselor uzuale de software și unelte de securitate. Cunoașterea arhitecturilor de sisteme de operare și platformelor necesare dezvoltării soluțiilor de securitate.<br>• C2.4 Identificarea și utilizarea unor criterii și metode adecvate pentru evaluarea, la diferite niveluri de abstractizare, a aplicațiilor informatice din punctul de vedere al securității acestora. Abilitatea de a evalua și documenta, din perspectiva securității, calitatea aplicațiilor informatice.<br>• C6.1 Înțelegerea arhitecturilor sistemelor de calcul și a modelelor de comunicare a acestora prin rețele. Abilitatea de a proiecta canale de comunicare solide din punctul de vedere al securității informațiilor transmise. |
| **Competenţe transversale** | • CT1 . Aplicarea și promovarea deprinderilor de proiectare și codare defensivă, sigură si eficientă. Îmbunătățirea abilităților profesionale prin valorificarea noii perspective dobândite, cea a securității sistemelor software. |

**7. Obiectivele disciplinei** (reieşind din grila competenţelor 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.<br>• Cunoașterea principalelor tipuri de vulnerabilități software, precum: utilizarea datelor utilizator nevalidate corespunzător, interacțiunea necontrolată directă sau indirectă cu mediul exterior aplicației etc.<br>• Deprinderea unor tehnici eficiente de studiere și evaluare a unui cod sursă din perspectiva securității și capacitatea de a identifica posibile vulnerabilități.<br>• Capacitatea de a evalua implicațiile unei vulnerabilități descoperite.<br>• Cunoașterea tehnicilor și a bibliotecilor de funcții utile în scrierea unui cod sursă fără vulnerabilități și capacitatea de a le utiliza în situații reale. |

**8. Conţinuturi**

| 8.1 Curs | | Metode de predare | Observaţii |
|---|---|---|---|
| 1 | 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, prezen tare cu video proiectorul, discuții, probleme scurte | |
| 2 | Vulnerabilități de corupere a memoriei ( *buffer/integer overflow etc.*) | | |
| 3 | Vulnerabilități specifice limbajului C: limite aritmetice (de reprezentare), conversii de tip, pointeri etc. | | |
| 4 | Vulnerabilități în componentele structurale ale unei aplicații software ( *Program building blocks*) | | |
| 5 | Vulnerabilități în utilizarea și manipularea șirurilor de caractere și metacaractere | | |
| 6 | Vulnerabilități specifice sistemelor de operare UNIX | | |
| 7 | Vulnerabilități specifice sistemelor de operare Windows | | |
| 8 | Vulnerabilități de sincronizare (în situații de concurență) | | |
| 9 | Vulnerabilități Web: injectare cod SQL, XSS, XSRF etc. | | |
| 10 | Vulnerabilități de criptografie: parole vulnerabile, numere aleatoare previzibile etc. | | |
| 11 | Vulnerabilități specifice codului aplicațiilor ce folosesc comunicarea în rețelele de calculatoare | | |
| 12 | Metode de proiectare corectă a aplicațiilor din perspectiva securității: principii de proiectare, definirea modelului de riscuri (threat modeling), evaluare design etc. | | |
| 13 | Metode de implementare corectă a unei aplicații software din perspectiva securității: metode și modele de dezvoltare a aplicațiilor (Waterfall, agile), cele mai frecvente și mai periculoase riscuri și vulnerabilități, tehnici de defensive de scriere a codului ( *defensive coding techniques*) | | |
| 14 | Metode de evaluare a (codului) unei aplicații din perspectiva securității: asigurarea calității, testare, gestiunea vulnerabilităților identificate | | |
| 8.2 Seminar / laborator | | Metode de predare | Observaţii |
| 1 | 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, tutoriale, ghiduri de lucru, demonstrații *live* | |

| | | | |
|---|---|---|---|
| 2 | Tehnici de evitare, detecție și evaluare a vulnerabilităților de corupere a memoriei si specifice limbajului C | ,explicații suplimentare, discuții, propunerea spre rezolvare a unor probleme de diferite tipuri și grade de complexitate. | |
| 3 | Tehnici de evitare, detecție și evaluare a vulnerabilităților de utilizare și gestionare a șirurilor de caractere și metacaractere | | |
| 4 | Tehnici de evitare, detecție și evaluare a vulnerabilităților specifice sistemului de operare Linux | | |
| 5 | Tehnici de evitare, detecție și evaluare a vulnerabilităților sistemelor de operare Windows | | |
| 6 | Tehnici de evitare, detecție și evaluare a vulnerabilităților de sincronizare | | |
| 7 | Tehnici de evitare, detecție și evaluare a ulnerabilităților aplicațiilor Web si aplicațiilor de rețea | | |

Bibliografie

1. M. Down, J. McDonald, J. Schuh, „ *The Art of Software Security Assessment. Identifying and Preventing Software Vulnerabilities* ”, AddisonWesley, 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* ”, AddisonWesley, 2006
5. R. Seacord, „CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems”, AddisonWesley, 2 nd edition, 2014
6. , „ *Common Weaknesses Enumeration* (WCE)”, online: http://cwe.mitre.org/data/index.html

**9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi 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 | Test online (grilă) sau lucrare scrisă (grilă), și/sau prezentarea unei | 50% |

| | | | |
|---|---|---|---|
| | nivel de cod sursă și de expunere a metodelor de evaluare și dezvoltare corectă a unui cod sursă din perspectiva securității.<br>· Abilitatea de rezolvare a unor probleme specifice domeniului.<br>· Prezență, (inter)activitate în timpul orelor de curs. | teme de cercetare din domeniul cursului. | |
| 10.5 Seminar/laborator | Abilitatea de rezolvare a unor probleme specifice domeniului<br>· 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 | 50% |
| 10.6 Standard minim de performanță | | | |
| • Capacitatea de a defini vulnerabilitățile software fundamentale, precum: bufferoverflow, injectare code SQL, XSS etc.<br>• Capacitatea de a identifica vulnerabilitățile software fundamentale și de a corecta codul (demonstrate în cadrul exercițiilor de laborator și a evaluării finale). | | | |

| Data completării | Titular de curs | Titular de seminar / laborator / proiect |
|---|---|---|
| 3.05.2017 | Lect. Dr. Mihai SUCIU | Drd. Raul TOȘA |

| Data avizării în departament | Director de departament |
|---|---|
| ..... | …..... |