FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea "Alexandru Ioan Cuza" din Iaşi**
1.2 Facultatea	**Facultatea de Informatică**
1.3 Departamentul	**Informatică**
1.4 Domeniul de studii	**Informatică**
1.5 Ciclul de studii	**Master**
1.6 Programul de studii / Calificarea	**Securitatea Informației**

2. Date despre disciplină

2.1 Denumirea disciplinei	**SECURITATE SOFTWARE**						
2.2 Titularul activităţilor de curs	**LECT. DR. CĂTĂLIN BÎRJOVEANU**						
2.3 Titularul activităţilor de seminar	**LECT. DR. CĂTĂLIN BÎRJOVEANU**						
2.4 An de studiu	**II**	**2.5** Semestru	**1**	**2.6** Tip de evaluare	**M**	**2.7** Regimul disciplinei*	**OB**

* *OB – Obligatoriu / OP – Opţional*

3. Timpul total estimat (ore pe semestru şi activităţi didactice)

3.1 Număr de ore pe săptămână	**4**	din care: **3.2** curs	**2**	**3.3** seminar/laborator	**2**
3.4 Total ore din planul de învăţământ	**56**	din care: **3.5** curs	**28**	**3.6** seminar/laborator	**28**

Distribuţia fondului de timp	ore
Studiu după manual, suport de curs, bibliografie şi altele	**30**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	**30**
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	**60**
Tutoriat	**-**
Examinări	**4**
Alte activităţi	**-**

3.7 Total ore studiu individual	**120**
3.8 Total ore pe semestru	**180**
3.9 Număr de credite	**8**

4. Precondiţii (dacă este cazul)

4.1 De curriculum	
4.2 De competenţe	

5. Condiţii (dacă este cazul)

5.1 De desfăşurare a cursului	-
5.2 De desfăşurare a seminarului/ laboratorului	**Prezența obligatorie la laborator**

6. Competenţe specifice acumulate

Competenţe profesionale	**C1.** Abilitatea de a explica principiile de securitate software si de a aplica principiile de securitate software pentru rezolvarea problemelor. **C2**. Abilitatea de a explica functionarea diferitelor mecanisme de securitate software si corelarea acestor mecanisme de securitate software cu principiile de securitate software. **C3.** Abilitatea de a compara diferitele mecanisme de securitate software și de a determina avantajele si limitările lor. C4. Abilitatea de a analiza si evalua sistemele software pentru proprietatile de securitate ale acestora.
Competenţe transversale	**CT1.** Capacitatea de a evalua riscurile sistemelor software. **CT2.** Capacitatea de a descrie diferite vulnerabilitati software.

7. Obiectivele disciplinei (din grila competenţelor specifice acumulate)

7.1 Obiectivul general	• Înțelegerea rolului pe care il are software-ul în asigurarea securității, dar și ca sursă de vulnerabilitati. • Înțelegerea amenințărilor și vulnerabilităților tipice care fac software-ul mai puțin sigur. • Înțelegerea cauzelor care stau la baza vulnerabilităților în software și cum acestea pot fi evitate. • Înțelegerea tehnicilor, principiilor și instrumentelor pentru a proiecta un soft mai sigur.
7.2 Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenţii vor fi capabili să: • detecteze vulnerabilităţile comune în software, • explice modul în care funcționează diverse atacuri, • să exploateze vulnerabilităţile comune în software, • proiecteze și sa implementeze mecanisme de securitate de bază pentru protejarea sistemelor software.

8. Conţinut

8.1	**Curs**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)
1.	Introducere în securitate software	Expunere	2
2.	Securitate in SDLC	Expunere	2
3.	Programe privilegiate Set-UID si atacuri asupra lor	Expunere	2
4.	Variabile de mediu si atacuri	Expunere	2
5.	Buffer Overflows	Expunere	2

6.	Atacuri bazate pe string-uri de format	Expunere	2
7.	Buffer Overflows: Atacuri si prevenire	Expunere	2
8.	Recapitulare	Dezbatere	2
9.	Atacuri Return-to-libc Race Condition	Expunere	2
10.	Limbaje de programare sigure	Expunere	2
11.	SQL Injection: Atacuri si prevenire	Expunere	2
12.	Atacuri Cross Site Scripting (XSS)	Expunere	2
13.	Prevenirea atacurilor Cross Site Scripting (XSS) Cross-Site Request Forgery (CSRF): Atacuri si prevenire	Expunere	2
14.	SandBoxing	Expunere	2

Bibliografie

- Wenliang Du, Computer Security: A Hands-on Approach, 2017.
- Ulfar Erlingsson, Yves Younan, Frank Piessens, Low-Level Software Security by Example, Springer, 2010.
- Justin Clarke, SQL Injection Attacks and Defense, 2nd Edition, Elsevier, 2012.
- Dafydd Stuttard, Marcus Pinto, The Web Application Hackers Handbook - Finding and Exploiting Security Flaws, 2nd Edition, John Wiley & Sons, October 2011.
- Michael Howard, David LeBlanc, John Viega, 24 Deadly Sins of Software Security, 2009.
- OWASP Top 10 Web Application Security Risks, 2017.
- CWE/SANS Top 25 Most Dangerous Programming Errors.

8.2	**Seminar / Laborator**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)
1.	Programe privilegiate Set-UID	Experiment, studii de caz, problematizare, exerciții	2
2.	Atacuri asupra programelor privilegiate Set-UID	Experiment, studii de caz, problematizare, exerciții	2
3.	Atacuri prin intermediul variabilelor de mediu	Experiment, studii de caz, problematizare, exerciții	2
4.	Atacul Shellshock	Experiment, studii de caz, problematizare, exerciții	2
5.	Atacuri Buffer Overflows	Experiment, studii de caz, problematizare, exerciții	2
6.	Atacuri bazate pe string-uri de format	Experiment, studii de caz, problematizare, exerciții	2
7.	Atacuri Return-to-libc	Experiment, studii de caz, problematizare, exerciții	2

8.	Atacuri Return-to-libc	Experiment, studii de caz, problematizare, exerciții	2
9.	Atacuri Race Condition	Experiment, studii de caz, problematizare, exerciții	2
10.	Atacuri SQL Injection	Experiment, studii de caz, problematizare, exerciții	2
11.	Atacuri Cross-Site Request Forgery (CSRF)	Experiment, studii de caz, problematizare, exerciții	2
12.	Atacuri Cross Site Scripting (XSS)	Experiment, studii de caz, problematizare, exerciții	2
13.	Atacuri Cross-Site Scripting (XSS) Scrierea XSS Worms	Experiment, studii de caz, problematizare	2
14.	Vulnerabilitati de securitate in sisteme software	Experiment, studii de caz, problematizare, exerciții	2

Bibliografie:

- Wenliang Du, Computer Security: A Hands-on Approach, 2017.
- Kali Linux Penetration Testing Platform, November, http://www.kali.org/
- OWASP Top 10 Web Application Security Risks, 2017.
- CWE/SANS Top 25 Most Dangerous Programming Errors.
- https://www.us-cert.gov/ncas/alerts/
- http://www.securitytracker.com/
- http://www.securityfocus.com/

9. Coroborarea conţinutului disciplinei cu aşteptările reprezentanţilor comunităţii, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului

Conținutul disciplinei este coroborat cu cerintele din companiile ce dezvolta solutii pentru securitatea sistemelor software.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală (%)
10.4 Curs	Înțelegerea vulnerabilităților software, a tehnicilor de exploatare a acestor vulnerabilități și a mecanismelor de securitate care pot fi aplicate pentru protectia sistemelor software.	Test scris	20%
10.5 Seminar/ Laborator	Analiza sistemelor software pentru găsirea vulnerabilităților de securitate, exploatarea vulnerabilităților și aplicarea tehnicilor care pot ajuta la	Exercitii pe parcursul laboratoarelor	80%

	prevenirea acestor atacuri.		
10.6 Standard minim de performanţă Simultan trebuie indeplinite conditiile: Test scris ≥ 5, Laborator ≥ 5			

Data completării
28.09.2018

Titular de curs
Lect. Dr. Cătălin Bîrjoveanu

Titular de seminar
Lect. Dr. Cătălin Bîrjoveanu

Data avizării în departament

Director de departament