



FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea “Alexandru Ioan Cuza” din Iași
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	Inginerie Software

2. Date despre disciplină

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

* OB – Obligatoriu / OP – Opțional

3. Timpul total estimat (ore pe semestru și activități 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 învățământ	56	din care: 3.5 curs	28	3.6 seminar/laborator	28
Distribuția fondului de timp					ore
Studiu după manual, suport de curs, bibliografie și altele					30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					30
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					60
Tutoriat					-
Examinări					4
Alte activități					-
3.7 Total ore studiu individual					120
3.8 Total ore pe semestru					180
3.9 Număr de credite					8

4. Precondiții (dacă este cazul)

4.1 De curriculum	
4.2 De competențe	

5. Condiții (dacă este cazul)

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



6. Competențe specifice acumulate

Competențe profesionale	<p>C1. Abilitatea de a explica principiile de securitate software și de a aplica principiile de securitate software pentru rezolvarea problemelor.</p> <p>C2. Abilitatea de a explica funcționarea diferitelor mecanisme de securitate software și corelarea acestor mecanisme de securitate cu principiile de securitate software.</p> <p>C3. Abilitatea de a compara diferitele mecanisme de securitate software și de a determina avantajele și limitările lor.</p> <p>C4. Abilitatea de a analiza și evalua sistemele software pentru proprietățile de securitate ale acestora.</p>
Competențe transversale	<p>CT1. Capacitatea de a evalua riscurile sistemelor software.</p> <p>CT2. Capacitatea de a descrie diferite vulnerabilități software.</p>

7. Obiectivele disciplinei (din grila competențelor specifice acumulate)

7.1 Obiectivul general	<ul style="list-style-type: none">• Înțelegerea rolului pe care îl are software-ul în asigurarea securității, dar și ca sursă de vulnerabilități.• 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	<p>La finalizarea cu succes a acestei discipline, studenții vor fi capabili să:</p> <ul style="list-style-type: none">• detecteze vulnerabilitățile comune în software,• explice modul în care funcționează diverse atacuri,• să exploateze vulnerabilitățile comune în software,• proiecteze și să implementeze mecanisme de securitate de bază pentru protejarea sistemelor software.

8. Conținut

8.1	Curs	Metode de predare	Observații (ore și referințe bibliografice)
1.	Introducere în securitate software	Expunere	2
2.	Securitate în SDLC	Expunere	2
3.	Bazele securității în Unix	Expunere	2
4.	Programe Set-UID și 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	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	Observații (ore și referințe bibliografice)
1.	Instrumente de analiza statica	Experiment, studii de caz, problematizare, exerciții	2
2.	Instrumente de analiza statica	Experiment, studii de caz, problematizare, exerciții	2
3.	Atacuri asupra programelor Set-UID	Experiment, studii de caz, problematizare, exerciții	2
4.	Variabile de mediu si atacuri	Experiment, studii de caz, problematizare, exerciții	2
5.	Atacul Shellshock	Experiment, studii de caz, problematizare, exerciții	2
6.	Atacuri Buffer Overflows	Experiment, studii de caz, problematizare, exerciții	2
7.	Atacuri bazate pe string-uri de format	Experiment, studii de caz, problematizare, exerciții	2



8.	Atacuri Return-to-libc	Experiment, studii de caz, problematizare, exerciții	2
9.	Web Tracking	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 conținutului disciplinei cu așteptările reprezentanților comunității, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului

Conținutul disciplinei este coroborat cu cerintele din companiile ce dezvoltă soluții 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 protecția 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	Exerciții pe parcursul laboratoarelor	80%



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

Data completării
7.05.2018

Titular de curs
Lect. Dr. Cătălin Bîrjoveanu

Titular de seminar
Lect. Dr. Cătălin Bîrjoveanu

Data avizării în departament

Director de departament