FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare si Tehnologia Informatiei
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informatiilor si Sistemelor de calcul/ Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	8.

2. Date despre disciplină

2.1 Denumirea disciplinei				***Securitate Web***	
2.2 Titularii de curs				Conf.dr.ing. Teodor ȘTEFĂNUȚ (teodor.stefanut@cs.utcluj.ro)	
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect				Conf.dr.ing. Teodor ȘTEFĂNUȚ (teodor.stefanut@cs.utcluj.ro)	
2.4 Anul de studiu	I	2.5 Semestrul	2	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	E
2.7 Regimul disciplinei	*DA – de aprofundare, DS – de sinteza, DC – complementară*				DA
	DI – Impusă, DOp – opțională, DFac – facultativă				DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	3	din care:	Curs	2	Seminar		Laborator	1	Proiect	
3.2 Număr de ore pe semestru	42	din care:	Curs	28	Seminar		Laborator	14	Proiect	
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										16
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										16
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										49
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activităţi:										0

3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))	83
3.5 Total ore pe semestru (3.2+3.4)	125
3.6 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Probleme de securitate la nivel de cod sursă
4.2 de competenţe	Programare web, Baze de date, Rețele de calculatoare

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

6. Competenţele specifice acumulate

6.1 Competenţe profesionale	C1 - Identificarea și înțelegerea problemelor de securitate ce pot apărea în diverse domenii de utilizare a sistemelor de calcul. Aplicarea adecvată a elementelor de bază ale managementului securității și ale modalităților de evaluare și management al riscurilor de securitate informatice • C1.1 – Cunoașterea noțiunilor, conceptelor și principiilor teoretice și practice avansate aferente domeniului general al securității informațiilor și sistemelor de calcul. Cunoașterea conceptelor aferente riscurilor, evaluării riscurilor și managementului securității • C1.2 – Înțelegerea riscurilor de securitate specifice unor situații noi și legătura lor cu cele cunoscute anterior. Prevederea scenariilor posibile de

	securitate, în momentul în care soluțiile de securitate cunoscute sunt folosite într-o situație sau domeniu nou • C1.3 – Modelarea unor noi tipuri de riscuri de securitate, evidențierea impactului asupra utilizatorului, asupra sistemelor și aplicațiilor existente. Identificarea unor soluții posibile și evaluarea lor • C1.4 – Stabilirea limitelor maxime de securitate oferite de soluții nou propuse. Plasarea corectă a riscurilor de securitate și a posibilelor soluții într-un cadru de repere bine cunoscute anterior • C1.5 – Elaborarea de modele teoretice noi de analiză a proprietăților de securitate sau evaluarea securității oferite de diverse soluții C3 - Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software • C3.1 – Cunoașterea teoretică și practică a diverselor scenarii de configurare sau mentenanță greșită a sistemelor de calcul, precum și a claselor de vulnerabilități software și atacuri informatice tipice • C3.2 – Analiza și înțelegerea unor protocoale de comunicare și module software noi, pentru identificarea unor vulnerabilități posibile. Utilizarea listelor dedicate, recunoscute în domeniu, de clase și tipuri de vulnerabilități și configurări greșite pentru analiza și validarea unui sistem informatic nou din punct de vedere al securității • C3.3 – Capacitatea de a analiza critic, din punctul de vedere al testării vulnerabilității, configurarea unei rețele, sistem de calcul sau aplicații software, fără să existe informații anterioare. Capacitatea de a identifica informații vizibile, servicii expuse etc. • C3.4 – Evaluarea limitărilor teoretice și practice oferite de diverse metode și tehnologii de detectare a vulnerabilităților și configurărilor greșite ale sistemelor de calcul. Determinarea unor corelări constructive între diverse metode de detecție • C3.5 – Propunerea unor noi metode de clasificare, identificare sau analiză pentru vulnerabilitățile și configurările greșite de sisteme. Crearea unor soluții și utilitare software care să identifice și analizeze astfel de cazuri C4 - Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate • C4.1 – Cunoașterea principiilor și noțiunilor de bază necesare dezvoltării și testării unui cod sigur din punctul de vedere al securității. Cunoașterea claselor uzuale de software și unelte de securitate. Cunoașterea arhitecturilor de SO și platformelor necesare dezvoltării soluțiilor de securitate • C4.2 – Identificarea de noi scenarii în care este nevoie de introducerea unei soluții de securitate sau utilizarea unei unelte de securitate. Analiza soluțiilor de securitate propuse și compararea lor cu cele cunoscute anterior • C4.4 – Evaluarea unor proiecte software existente și identificarea greșelilor de securitate din punctul de vedere al arhitecturii, modului de programare sau procedurilor de testare. Propunerea unor noi metode de dezvoltare și testare
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Înțelegerea vulnerabilităților comune prezente în aplicațiile Web, a modului în care acestea pot fi exploatate cu intenții malițioase și a tehnicilor de dezvoltare, instalare și configurare a aplicațiilor Web securizate
7.2 Obiectivele specifice	1. Înțelegerea modului de funcționare a aplicațiilor Web 2. Dezvoltarea abilității de a identifica vulnerabilități în implementarea aplicațiilor Web 3. Înțelegerea tehnicilor de exploatare a vulnerabilităților aplicațiilor Web (XSS, SQL injection etc.)

	4. Dezvoltarea aptitudinilor de scriere de cod securizat pentru aplicațiile Web 5. Dezvoltarea aptitudinilor de configurarea corectă a aplicațiilor Web, din perspectiva securității

8. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Privire de ansamblu asupra tehnologiilor Web (1): concepte generale (clienți/servere, web 2.0, DOM etc.), arhitectura aplicațiilor web (frontend/middleware/backed)	2	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Privire de ansamblu asupra tehnologiilor Web (2): protocoale (stiva ISO-OSI, HTTP, FTO, TCP, SOAP etc.) și limbaje (HTML, CSS, SVG, JS, XML, JSON, PHP, Python, Ruby etc.)	2		
Securitatea Web (1): autentificare (identitate), autorizare, criptare și legislație în domeniu	2		
Securitatea Web (2): confidențialitate, integritate și disponibilitate, nivelul rețea (firewalls, IPS)	2		
Securitatea serverelor (1): vulnerabilități și atacuri (OWASP, atacuri prin injecții SQL/hijack de sesiune/SSL/referințe directe de obiecte/etc.)	2		
Securitatea serverelor (2): asigurarea disponibilității (atacul (D)DoS) și configurarea corectă	2		
Securitatea clienților (browser-e Web) (1): vulnerabilități (browser, pluginuri Flash/Java/etc., cookies, DNS, clickjacking)	2		
Securitatea clienților (browser-e Web) (2): configurare, sandboxing, scripturi utilizator, malware/spyware	2		
Criptografie pentru Web: concepte generale, chei publice/private, certificate, integritatea mesajelor, protocoale (SSL, HTTPS etc.)	2		
Măsuri proactive de securitate: detectarea intruziunilor în aplicații web, gestionarea de incidente, honeytokens	2		
Securitatea pentru Web 2.0: paradigma AJAX, cloud computing etc.	2		
Programare sigură pentru Web (1): validarea intrărilor/sanitizarea erorilor, identitatea, controlul accesului, gestionarea sesiunilor	2		
Programare sigură pentru Web (2): gestionarea datelor cu sensibilitate mare, practici corecte de programare	2		
Prezentare de sinteză a subiectelor studiate, evidențierea concluziilor importante, discutarea unor subiecte propuse de studenți	2		

Bibliografie *(bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziţia studenţilor într-un număr de exemplare corespunzător)*

1. 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)
2. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)
3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)
4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)
5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)
6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)
7. Diferite articole și site-uri Web

8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Dezvoltarea unei aplicații minimale Web (frontend/middleware/backend)	1	Expunere la tablă, explicații suplimentare, discuții, exerciții de laborator	
Analiza de pachete de rețea în protocoale Web, implementarea / configurarea unui firewall	1		
Analiza atacurilor Web: OWASP, vulnerabilități de sesiune, injecții SQL	1		
Analiza atacurilor Web: XSS, CSRF, referințe directe nesecurizate, SSL	1		

Analiza și exploatarea de vulnerabilități în browser-ele Web: JavaScript, traversare de path-uri si în plugin-uri de browser-e Web (Flash, Java etc.)	1		
Programare sigură: validarea intrărilor, evitarea expunerii publice a detaliilor cazurilor de eroare, tratarea datelor sensibile, practici corecte etc.	1		
Utilizarea instrumentelor de validare a site-urilor Web: scannere de vulnerabilități cunoscute si fuzzere	1		

Bibliografie *(bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziţia studenţilor într-un număr de exemplare corespunzător)*

1. 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)
2. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)
3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)
4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)
5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)
6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)
7. Diferite articole și site-uri Web

*Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.

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

Se realizează prin discuții periodice cu reprezentanți ai angajatorilor semnificativi, în special cei care angajează pe proiecte din domeniul securității informațiilor.
Cursuri de securitate web sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, cum ar fi:

- XACS241 - Web Security 2.0 (Stanford) – http://scpd.stanford.edu/search/publicCourseSearchDetails.do?method=load&courseId=1284858
- 06-20009 Network Security (University of Birmingham) – http://www.cs.bham.ac.uk/internal/modules/2010/20009/
- Internet and Security (Nottingham University) – http://targetpostgrad.com/course/31312-internet-and-security
- Master of Science in Cybersecurity (University of Maryland) – http://www.umuc.edu/academic-programs/masters-degrees/cybersecurity.cfm
- Applied Cyber Security (MIT) – http://web.mit.edu/professional/short-programs/courses/applied_cyber_security.html

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs	Examen scris și/sau tip grilă și/sau oral și/sau prezentarea unei teme de cercetare din domeniul cursului. Susținerea va fi organizată față-în-față sau online.	50%
Seminar			
Laborator	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de laborator	Realizarea activităților de laborator și rezolvarea temelor de casă și/sau a unor probleme în cadrul unui examen practic. Examen grilă pentru verificarea fixării noțiunilor de bază, susținut pe hârtie sau suport electronic și organizat față-în-față sau online.	50%
Proiect			

Standard minim de performanţă:
Curs. Prezența la **minimum 50%** din orele de curs, pentru admiterea la examenul final. Capacitatea de a explica și defini conceptele elementare de securitate a aplicațiilor Web (SQL injection, XSS, CSRF, configurare) și a riscurilor la care sunt expuse datele și aplicațiile publicate pe Web.
Aplicații. Prezența la laborator **obligatorie 100%** (1 laborator se poate recupera în timpul semestrului, iar altul în sesiunile de restanțe) pentru admiterea la examenul final. Capacitatea de a identifica vulnerabilități de bază (SQL injection, XSS, CSRF, de configurare) în codul sursă al aplicațiilor web. Capacitatea de a scrie cod securizat pentru aplicații Web de complexitate mică.

Data completării:	**Titulari**	**Titlu Prenume NUME**	**Semnătura**
	Curs	Conf.dr.ing. Teodor ȘTEFĂNUȚ	
	Aplicații	Conf.dr.ing. Teodor ȘTEFĂNUȚ	

Data avizării în Consiliul Departamentului Calculatoare	Director Departament Prof.dr.ing. Rodica Potolea
Data aprobării în Consiliul Facultății de Automatică și Calculatoare	Decan Prof.dr.ing. Liviu Miclea