A TANTÁRGY ADATLAPJA

1. A képzési program adatai

1.1 Felsőoktatási intézmény	Babeş-Bolyai Tudományegyetem
1.2 Kar	Matematika és Informatika
1.3 Intézet	Magyar Matematika és Informatika
1.4 Szakterület	Informatika
1.5 Képzési szint	Alap
1.6 Szak / Képesítés	Informatika

2. A tantárgy adatai

2.1 A tantárgy neve	**Szoftver biztonság** Securitate software – Secure coding						
A tantárgy kódja:	**MLM5086**						
2.2 Az előadásért felelős tanár neve	Robu Judit						
2.3 A szemináriumért felelős tanár neve	Fülöp Botond (Bitdefender)						
2.4 Tanulmányi év	3	2.5 Félév	5	2.6 Értékelés módja	kollok-vium	2.7 Tantárgy típusa	választható szak

3. **Teljes becsült idő** (az oktatási tevékenység féléves óraszáma)

3.1 Heti óraszám	4	melyből: 3.2 előadás	2	3.3 labor/projektr	1+1
3.4 Tantervben szereplő össz-óraszám	56	melyből: 3.5 előadás	28	3.6 labor/projektr	28
A tanulmányi idő elosztása:					óra
A tankönyv, a jegyzet, a szakirodalom vagy saját jegyzetek tanulmányozása					13
Könyvtárban, elektronikus adatbázisokban vagy terepen való további tájékozódás					8
Szemináriumok / laborok, házi feladatok, portofóliók, referátumok, esszék kidolgozása					23
Egyéni készségfejlesztés (tutorálás)					0
Vizsgák					0
Más tevékenységek:					

3.7 Egyéni munka össz-óraszáma	44
3.8 A félév össz-óraszáma	100
3.9 Kreditszám	4

4. **Előfeltételek** (ha vannak)

4.1 Tantervi	• Nincsen
4.2 Kompetenciabeli	• C programozási készség, x86 architektúra ismerete, alap webprogramozás és SQL ismeretek

5. **Feltételek** (ha vannak)

5.1 Az előadás lebonyolításának feltételei	• Táblával és videoprojektorral felszerelt előadó
5.2 A szeminárium / labor / projekt lebonyolításának feltételei	• Számítógépes terem

6. Elsajátítandó jellemző kompetenciák

Szakmai kompetenciák	**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. **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. **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. **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. **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. **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.
Transzverzális kompetenciák	**CT1** Aplicarea și promovarea deprinderilor de proiectare defensivă, sigură si eficientă. Îmbunătățirea abilităților profesionale prin valorificarea noii perspective dobândite, cea a securității sistemelor software.

7. **A tantárgy célkitűzései** (az elsajátítandó jellemző kompetenciák alapján)

7.1 A tantárgy általános célkitűzése	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 A tantárgy sajátos célkitűzései	• Cunoaşterea mecanismelor de bază ce definesc securitatea sistemului şi 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. • Cunoaşterea principalelor tipuri de vulnerabilităşi software, precum: utilizarea datelor utilizator nevalidate corespunzător, interacțiunea necontrolată directă sau indirectă cu mediul exterior aplicației etc. • Deprinderea unor tehnici eficiente de studiere şi evaluare a unui cod sursă din perspectiva securității şi capacitatea de a identifica posibile vulnerabilități. • Capacitatea de a evalua implicațiile unei vulnerabilități descoperite. • Cunoaşterea tehnicilor şi a bibliotecilor de funcții utile în scrierea unui cod sursă fără vulnerabilități şi capacitatea de a le utiliza în situații reale.

8. A tantárgy tartalma

8.1 Előadás	Didaktikai módszerek	Megjegyzések
1. Szoftver biztonsági rések, biztonságos szoftverfejlesztés, biztonság kiértékelése.	Problémafelvetés, előadás, megbeszélés	
2. Memória sebezhetőség (puffer/integer túlcsordulás, stb)		
3. C-specifikus sebezhetőségek: numerikus adatok ábrázolása, határok, típuskonverziók, mutatók, stb.		
4. Szoftver alkalmazások alkotóelemeihez kacsolódó sebezhetőségek.		
5. Karaktersorokkkal és metakarakterekkel kapcsolatos sebezhetőségek.		
6. UNIX operációs rendszerekhez kapcsolódó sebezhetőségek.		
7. Windows operációs rendszerekhez kapcsolódó sebezhetőségek.		
8. Szinkronizálás, versenyhelyzet		
9. Webes alkalmazások sebezhetősége: SQL injection, XSS, XSRF, stb.		
10. Kriptográfiai sebezhetőségek: feltörhető jelszavak, megjósolható véletlen számok, stb.		
11. Hálózati kommunikációhoz kapcsolódó sebezhetőségek.		
12. Alkalmazások helyes tervezése, biztonsági megközelítés: alapelvek, fenyegetési modell, kiértékelés		
13. Alkalmazások biztonságkritikus implementálása (defensive coding techniques)		
14. Kód ellenőrzés, tesztelés, beazonosított sebezhetőségek kezelése		

Könyvészet

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. R. Anderson, *Security Engineering,* Wiley, ^{2}2008.
4. C. P. Pfleeger, S. L. Pfleeger, J. Margulies: *Security in Computing*, Prentice Hall, ^{5}2015.
5. M. Howard, D. LeBlanc, *Writing Secure Code for Windows Vista*, Microsoft Press, 2007
6. G. McGraw, *Software Security:Building Security In*, Addison-Wesley, 2006
7. R. Seacord, *CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems*, Addison-Wesley, ^{2}2014
8. -, *Common Weaknesses Enumeration(WCE)*, on-line: http://cwe.mitre.org/data/index.html

8.2 Szeminárium / Labor / Projekt	Didaktikai módszerek	Megjegyzések
1. Kódbeli sebezhetőségek beazonosítására használatos eszközök	Elméleti összefoglaló, sebezhetőségek gyakorlati bemutatása, egyéni munka	
2. Memória sebezhetőség		
3. A **C** nyelv sebezhetősége		
4. String-ek és metakarakterek		
5. Linux biztonsági rések		
6. Windows biztonsági rések		
7. Webes biztonsági rések		

9. A tantárgy tartalmának összhangba hozása az episztemikus közösségek képviselői, a szakmai egyesületek és a szakterület reprezentatív munkáltatói elvárásaival.

- A tantárgy tartalma megegyezik az egyetemi oktatásban a fontosabb egyetemeken oktatott „Software Security” tárgy hagyományos tartalmával.

10. Értékelés

Tevékenység típusa	10.1 Értékelési kritériumok	10.2 Értékelési módszerek	10.3 Aránya a végső jegyben
10.4 Előadás	Alapfogalmak ismerete	Quiz	20 %
10.5 Szeminárium / Labor	Laborfeladatok,	Minden héten gyakorlati feladatok, a félév végén összefoglaló gyakorlati feladat: sebezhetőségek azonosítása és javítása 2 programban	80 %
10.6 A teljesítmény minimumkövetelményei			
• Laborfeladatok elkészítése, átmenő jegy elméleti és gyakorlati felmérőn.			

Kitöltés dátuma	Előadás felelőse	Szeminárium felelőse
2016.04.25.	dr. Robu Judit docens	Fülöp Botond, Bitdefender

Az intézeti jóváhagyás dátuma

……

Intézetigazgató,

Dr. András Szilárd, egyet. docens