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	Számítógépek és információ-technológia
1.5 Képzési szint	Alapképzés
1.6 Szak / Képesítés	Információmérnöki (magyar nyelven)

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	Robu Judit						
2.4 Tanulmányi év	3	2.5 Félév	5	2.6 Értékelés módja	kollok-vium	2.7 Tantárgy típusa	választható szaktárgy

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

3.1 Heti óraszám	4	melyből: 3.2 előadás	2	3.3 labor/projektr	2
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					18
Könyvtárban, elektronikus adatbázisokban vagy terepen való további tájékozódás					23
Szemináriumok / laborok, házi feladatok, portofóliók, referátumok, esszék kidolgozása					23
Egyéni készségfejlesztés (tutorálás)					5
Vizsgák					0
Más tevékenységek:					

3.7 Egyéni munka össz-óraszáma	69
3.8 A félév össz-óraszáma	125
3.9 Kreditszám	5

4. **Előfeltételek** (ha vannak)

4.1 Tantervi	• Számítógép architektúra • Operációs rendszerek • Adatszerkezetek • Adatbázisok • Webprogramozás
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** A programozási paradigmák és a specifikus nyelvi mechanizmusok megfelelő leírása, valamint a szemantikai és a szintaktikai vonatkozások közötti különbség meghatározása **C1.2** A meglévő szoftveralkalmazások magyarázata absztrakciós szintek szerint (architektúra, csomagok, osztályok, metódusok) az alapismeretek használatával **C1.4** Alkalmazások tesztelése adott tesztelési terv alapján. **C2.1** A szoftverrendszerek megfelelő fejlesztési módszereinek beazonosítása. **C2.4** Megfelelő kritériumok és módszerek használata az alkalmazások értékeléséhez. **C6.1** Számítási rendszerek és számítógépes hálózatok alapkoncepcióinak és modelleinek azonosítása
Transzverzális kompetenciák	**CT1** A szervezett és hatékony munka szabályainak, a didaktikai-tudományos területhez való felelősségteljes hozzáálll

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

7.1 A tantárgy általános célkitűzése	Capacitatea evaluării caracteristicilor de securitate ale unei aplicaţii software la nivelul codului sursă. Dobândirea deprinderilor fundamentale minimale de scriere a unui cod sursă fără vulnerabilităţi.
7.2 A tantárgy sajátos célkitűzései	• Cunoaşterea mecanismelor de bază ce definesc securitatea sistemului şi a mediului software în care se execută o aplicaţie (i.e. modelul de securitate), cum ar fi: permisiunile de acces, politicile de securitate, interacţiunea cu mediul exterior etc. • Cunoaşterea principalelor tipuri de vulnerabilităţi software, precum: utilizarea datelor utilizator nevalidate corespunzător, interacţiunea necontrolată directă sau indirectă cu mediul exterior aplicaţiei etc. • Deprinderea unor tehnici eficiente de studiere şi evaluare a unui cod sursă din perspectiva securităţii şi capacitatea de a identifica posibile vulnerabilităţi. • Capacitatea de a evalua implicaţiile unei vulnerabilităţi descoperite. • Cunoaşterea tehnicilor şi a bibliotecilor de funcţii utile în scrierea unui cod sursă fără vulnerabilităţi şi capacitatea de a le utiliza în situaţii 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, A Guide to Building Dependable Distributed Systems,* Wiley, [3]2020. https://www.cl.cam.ac.uk/~rja14/book.html
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
9. -, ICS – CERT Advisories, on-line: https://www.cisa.gov/uscert/ics/advisories

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
2022.04.25.	dr. Robu Judit docens	dr. Robu Judit docens

Az intézeti jóváhagyás dátuma	Intézetigazgató,
2022.04.30.	Dr. András Szilárd, egyet. docens