BLG460E – SECURE PROGRAMMING

2021-2022 SPRING

Time & Place:	On Tuesday afternoons, at 15:30, in EEB 5304
Instructor:	Dr. Mehmet Tahir SANDIKKAYA sandikkaya@itu.edu.tr EEB 5310
Teaching Assistant:	Ayşe SAYIN sayinays@itu.edu.tr EEB 5211

Weekly Plan

W	Date	Topic	Coverage	Announcements	Submissions
1	22 Feb	Fundamental concepts of security	7	TP-A	
2	01 Mar	Compilation and Execution	1, 7		
3	08 Mar	Stack overflow and its mitigation	1, 7	HW1-A	
4	15 Mar	Dynamic memory management	1, 7		
5	22 Mar	Canonicalization attacks and mitigation*	3, 7	HW2-A	HW1-S
6	29 Mar	Injection attacks	2, 7	HW1-G	
7	05 Apr	Injection mitigation*	2, 7	HW3-A	HW2-S
8	12 Apr	Reverse engineering and obfuscation	7	HW2-G	
9	19 Apr	Fundamental cryptography	4		HW3-S
10	26 Apr	Principles of computer networks*	5	HW3-G	MT
11	10 May	XSS & CSRF attacks and mitigation	5	HW4-A	
12	17 May	Race conditions*	5	MT-G	
13	24 May	Permission and authorization mechanisms in contemporary languages	6		HW4-S
14	31 May	Test and static analysis tools	7	HW4-G	TP-S

(*) Recitations

Textbook

Textbook	David A. Wheeler, "Secure Programming HOWTO", version 3.71, 2015. (https://dwheeler.com/secure-programs/)
Other References	Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland, David Svoboda, "Java Coding Guidelines 75 Recommendations for Reliable and Secure Programs", Addison-Wesley, 2014. (ISBN: 978-0321933157) Robert C. Seacord, “Secure Coding in C and C++”, 2nd ed., Addison-Wesley, 2013. (ISBN: 978-0321822130) Jon Erickson, “Hacking: The Art of Exploitation”, 2nd ed., No Starch Press, 2008. (ISBN: 978-1593271442) Michael Howard, David LeBlanc, “Writing Secure Code: Practical Strategies and Proven Techniques for Building Secure Applications in a Networked World”, Microsoft Press, 2004. (ISBN: 978-0735617223)

Grades

- Quiz: 10%
- Homework: 4×6% = 24%
- Term Project: 10% (optional)
- Mid-term: 26%
- Final: 40%

Grading

- ∑HW ≥ 7/24 (otherwise VF)
- (MT+Q+TP+∑HW) ≥ 24/70 (otherwise VF)
- (F+MT+Q+TP+∑HW) ≥ 40/100 (otherwise FF)

Important Notes

- **Classroom Announcements**: You are expected to know everything that was announced in the classroom. There does not necessarily have to be an announcement on Ninova. If you have missed a class, ask your classmates if there were any announcements that you need to know.
- **Ninova**: You need to follow the course announcements, attendance, and check your exam results on Ninova (https://ninova.itu.edu.tr/). You are responsible to check the Ninova site regularly for updates.
- **ITU Email Accounts**: Course related e-mail notifications will be sent to your ITU account; you are responsible to check it regularly.
- **Email Etiquette**: When sending e-mail to the instructors or assistants, use your ITU account. Your full name must appear in the body of the e-mail. The e-mail subject must be or at least include "BLG 460E". Do not send the same e-mail repeatedly or to multiple recipients. It will be handled in the best available time. Your e-mails may be in English or Turkish. Regardless of which language you use, use proper grammar, lowercase/uppercase letters, and punctuation. Your e-mails should not look like chat messages. It should include a proper subject line, greeting, the matter of your communication and your signature at the end. Prefer your ITU e-mail account as public accounts are useless to prove your genuine identity.
- **Recitations**: You will be responsible for organizing yourselves for recitations and exercises; you may either work alone or better form (online) groups.
- **Provided Software**: Assignments require use of certain software packages. It is your job to acquire this software to use on a personal computer. However, a software "image" containing an operating system with this software installed, that can be loaded onto a bootable memory stick, will be provided to ease this task.
- **Notes**: Although resources are provided, you are expected to take notes during the lectures. This is important for your learning both of the topic and of how to acquire and organize information.
- **Collaboration**: There are no group assignments in this course unless otherwise stated. Homework in this course consists of individual assignments. In other words, collaboration on these assignments is not allowed. You are encouraged to help your classmates understand the material, but you should refrain from discussing any issues specific to the assignment. You should definitely not share any homework documents for any reason with anybody, or else, should not copy anything from anybody.
- **Timeliness**: Be sure to budget sufficient time to complete assignments before the deadline. Late submissions will not be allowed. Submissions via e-mail cannot be accepted as there will be no official trace of your work on Ninova. Upload your work incrementally on Ninova even if it is not yet complete. Do not wait for the last minute.
- **Plagiarism**: Any form of cheating or plagiarism will not be tolerated. This includes actions such as, but not limited to, submitting the work of others as one's own (even if in part and even with modifications), and providing work for others to submit. **Serious offences will be reported to the faculty administration for disciplinary measures**. See (translate if required) https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=16532&MevzuatTur=7&MevzuatTertip=5
- **Ethics**: Please carefully read the following document prepared by the Student Affairs Office: (translate if required) https://odek.itu.edu.tr/etik-ilkelerimiz/akademik-onur-sozu
- **Accountability:** You accept the course specific rules and conditions by registering to this class; so that, you are accordingly accountable for your further behavior.