ITU
DERS KATALOG FORMU
(Course Catalogue Form)

Dersin Adı: Güvenli Programlama	**Course Name:** Secure Programming

Kodu (Course Code)	**Yarıyıl (Semester)**	**Kredisi (Local Credits)**	**AKTS Kredisi (ECTS Credits)**	**Ders Uygulaması, Saat/Hafta**		
				Ders (Theoretical)	**Uygulama (Tutorial/Recitation)**	**Laboratuvar (Laboratory)**
BLG460E	8	2	4	2	-	-

Bölüm/Program (Department/Program)	Bilgisayar Mühendisliği / Computer Engineering

Dersin Türü (Course Type)	Mühendislik Tasarım (Engineering Design)	**Dersin Dili (Course Language)**	İngilizce (English)
Ders Zorunluluğu (Course Compulsion)		Seçmeli (Elective)	

Dersin Önkoşulları (Course Prerequisites)	BLG252E Object Oriented Programming			
Dersin Mesleki Bileşene Yüzde Katkısı (Course Category by Content Percentage)	Temel Bilim (Basic Science)	Temel Mühendislik (Engineering Science)	Mühendislik Tasarım (Engineering Design)	İnsan ve Toplum Bilim (General Education)
	0%	20%	80%	0%

Dersin İçeriği (Course Description)	Yazılımda güvenliği etkileyen hataların belirlenmesi ve giderilmesi, Yığın taşırma saldırıları, Komut iliştirme saldırıları, Ters mühendislik ve kod perdeleme yöntemleri, İnternet yörelerine yapılan saldırılar, Programlama dillerinde izin ve yetkilerin kullanımı, Temel kriptolojik işlevler ve bunların bilgisayar haberleşmesinde uygulanması, Temel işletim sistemi görevleri ve yazılım güvenliğini etkileyen yanları
	Determining and mitigating programming mistakes that may affect software security, Stack overflow attacks, Injection attacks, Reverse engineering and code obfuscation, Attacks that target web sites, Handling permissions and authorization in programming languages, Basic cryptologic functions and their usage in computer communications, Basic operating system duties and its effect on

	software security
Dersin Amacı (Course Objective)	1. Bir yazılımın gerçeklenmesi sırasında karşılaşılabilecek güvenlik sorunlarını öğretmek. 2. Bilinen saldırılardan etkilenmeyen yazılımlar geliştirmeyi öğretmek. 3. Uygun programlama alışkanlıkları kazandırılarak yeni saldırılardan olabildiğince az etkilenecek yazılımlar geliştirmeyi öğretmek. 4. Güvenli bir yazılım ortaya koymak için gerekli teknik becerileri ve düşünce yapısını kazandırmak.
	1. Teaching possible security flaws that may be encountered during software implementation. 2. Students can produce software that does not be affected by known development-time vulnerabilities. 3. Students will gain defensive development style to be less affected by future development-time vulnerabilities. 4. Students will gain the technical abilities to produce secure software.
Dersin Öğrenme Çıktıları (Course Learning Outcomes)	1. Bellek sızmalarına dirençli program yazabilirler. 2. Beklenmedik girişlerin güvenliği bozucu etkilerine karşı yazdıkları programları koruyabilirler. 3. Standart dışılıkları düzenleyerek güvenlik sağlama yöntemlerini bilirler. 4. Yazdıkları kaynak kodları perdeleyebilirler. 5. İnternet'te sık karşılaşılan saldırılara karşı önlem alarak kod yazabilirler. 6. İzinlerin ve yetkilendirmenin nasıl kullanılacağını bilirler. 7. Güvenli programlama stili kazanarak olası sorunlara dirençli yazılımlar oluşturabilirler.
	1. Write programs who can resist memory overflows. 2. Protect the programs they write against the improbable effects of malicious user input. 3. Know the protection by sanitizing non-standard components. 4. Obfuscate their code. 5. Write programs against well-known Internet vulnerabilities. 6. Know how to use permissions and authorization. 7. Obtain defensive programming style to mitigate future vulnerabilities.

Ders Kitabı (Textbook)	David A. Wheeler, "Secure Programming HOWTO", version 3.71, 2015. (https://dwheeler.com/secure-programs/)
Diğer Kaynaklar (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)

Ödevler ve	Üç ödev ve bir proje tamamlanacaktır.

Projeler (Homeworks & Projects)	There will be three homework assignments and one term project.
Laboratuvar Uygulamaları (Laboratory Work)	-
	-
Bilgisayar Kullanımı (Computer Use)	Ödevlerin ve projenin tamamlanması için öğrenciler kişisel bilgisayara gereksinir. Alıştırma yapılabilecek sanal bilgisayar imajı sağlanacaktır.
	Students require a personal computer to complete the homework assignments and the term project. A virtual machine image will be provided for exercises.
Diğer Uygulamalar (Other Activities)	-
	-

Başarı Değerlendirme Sistemi (Assessment Criteria)	**Faaliyetler (Activities)**	**Adedi (Quantity)**	**Değerlendirmedeki Yüzde Katkısı (Effects on Grading by Percentage)**
	Yıl İçi Sınavları (Midterm Exams)	2	50%
	Kısa Sınavlar (Quizzes)	1	10%
	Ödevler (Homework)	3	15%
	Projeler (Projects)	1	25%
	Dönem Ödevi/Projesi (Term Paper/Project)	-	-
	Laboratuvar Uygulaması (Laboratory Work)	-	-
	Diğer Uygulamalar (Other Activities)	-	-
	Final Sınavı (Final Exam)	-	-

DERS PLANI
(Course Plan)

Hafta	**Konu**	**Dersin Çıktıları**

1	Güvenliğin temel kavramları	7
2	Yığını taşırma saldırıları ve korunma yolları (1/2)	1, 7
3	Yığını taşırma saldırıları ve korunma yolları (2/2)	1, 7
4	Dinamik bellek yönetimi	1, 7
5	Kanonik yazım saldırıları ve korunma yolları	3, 7
6	Komut iliştirme saldırıları ve korunma yolları (1/2)	2, 7
7	Komut iliştirme saldırıları ve korunma yolları (2/2)	2, 7
8	Uygulamalı saldırılardan örnekler ve çözümler	7
9	Ters mühendislik ve kod perdeleme yöntemleri	4
10	Kriptolojinin temelleri, bilgisayar haberleşmesi ilkeleri	5
11	XSS, CSRF saldırıları ve korunma yolları	5
12	Yarış durumları	5
13	Güncel programlama dillerinde izinlerin ve yetkilerin kullanımı	6
14	Sınama ve yerinde çözümleme araçları	7

Week	**Topic**	**Course Outcome**
1	Fundamental concepts of security	7
2	Buffer overflow attacks and defenses (1/2)	1, 7
3	Buffer overflow attacks and defenses (2/2)	1, 7
4	Dynamic memory management	1, 7
5	Canonicalization attacks and defenses	3, 7
6	Injection attacks and defenses	2, 7
7	Injection attacks and defenses	2, 7
8	Applied attack examples and their solutions	7
9	Reverse engineering and obfuscation methods	4
10	Basics of cryptology, principles of computer communication	5
11	XSS & CSRF attacks and defenses	5
12	Race conditions	5
13	Permission and authorization mechanisms in contemporary languages	6
14	Test and static analysis tools	7

DERSİN BİLGİSAYAR MÜHENDİSLİĞİ ÖĞRENCİ ÇIKTILARI İLE İLİŞKİSİ
Relationship between the Course and Student Outcomes
(1: "Little", 2: "Partial", 3: "Full", Leave blank if your answer is "None")

Computer Engineering Department Program Outcomes and Performance Criteria		Level of Contribution		
		1	2	3
1	an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics			X
2	an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors		X	
3	an ability to communicate effectively with a range of audiences		X	
4	an ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts			X
5	an ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives			X
6	an ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions	X		
7	an ability to acquire and apply new knowledge as needed, using appropriate learning strategies			X

HAZIRLANMA BİLGİSİ
Edition Information

Prepared by	Date	Signature
Mehmet Tahir SANDIKKAYA	**2020-12-04**	**MTS**
Approved by	**Date**	**Signature**