Jordan University of Science and Technology

Faculty of Computer & Information Technology

Cybersecurity Department

CY431 Software Security - JNQF Level: 7

First Semester 2024-2025

Course Catalog
3 Credit Hours. Theory and practice of software security, focusing in particular on some common software security risks, including buffer overflows, race conditions and random number generation, and on identification of potential threats and vulnerabilities early in design cycle. Emphasizes methodologies and tools for identifying and eliminating security vulnerabilities, techniques to prove absence of vulnerabilities, ways to avoid security holes in new software, and essential guidelines for building secure software: how to design software with security in mind from the ground up and to integrate analysis and risk management throughout the software life cycle.
Teaching Method: Blended

Text Book	
Title	Software Security: Principles, Policies, and Protection
Author(s)	Mathias Payer
Edition	1st Edition
Short Name	Ref #1
Other Information	

Course References

Short name	Book name	Author(s)	Edition	Other Information
Ref #2	Software Security: Building Security In	Gary McGraw. Addison-Wesley	1st Edition	ISBN 978-321-35670-3

Instructor	
Name	**Dr. Heba Alawneh**
Office Location	-

Office Hours	Sun : 08:30 - 10:30 Tue : 12:30 - 13:30 Wed : 08:30 - 09:30 Thu : 08:30 - 10:30
Email	hzalawneh@just.edu.jo

Class Schedule & Room

Section 1:
Lecture Time: Sun, Tue : 10:30 - 11:30
Room: M2008

Section 2:
Lecture Time: Tue, Thu : 11:30 - 12:30
Room: M2202

Prerequisites

Line Number	Course Name	Prerequisite Type
1773440	CY344 Networks Security Laboratory	Prerequisite / Study
1772110	CY211 Selected Visual Programming Language	Prerequisite / Study
1774520	CY452 Web Security	Pre./Con.

Tentative List of Topics Covered

Weeks	Topic	References
Weeks 1, 2	Software Security Basic Principles	From **Ref #1**
Weeks 3, 4	Secure Software Lifecycle	From **Ref #1**
Weeks 3, 4	Secure Software Lifecycle	From **Ref #1**
Week 5	Security Policies	From **Ref #1**
Week 6	Software Vulnerabilities	From **Ref #1**, From **Ref #2**
Week 7	Attack Vectors	From **Ref #1**
Weeks 8, 9	Mitigations	From **Ref #1**
Weeks 10, 11	Testing	From **Ref #1**
Weeks 12, 13	Assessing Software Security	From **Ref #1**

Mapping of Course Outcomes to Program Outcomes and NQF Outcomes	Course Outcome Weight (Out of 100%)	Assessment method
Understand the fundamental principles of software security, including confidentiality, integrity, and availability. [1SO1] [1L7K1]	20%	

Identify common security threats, risks, and attack vectors for software systems. [1SO2] [1L7S1]	25%	
Evaluate secure coding practices and software development lifecycle (SDLC) methodologies to mitigate security risks. [1SO4] [1L7S2]	25%	
Assess various defense mechanisms and security policies to protect software systems. [1SO6] [1L7C4]	20%	
Identify security problems in a given source code or application. [1SO5] [1L7C1]	10%	

Relationship to Program Student Outcomes (Out of 100%)					
SO1	SO2	SO3	SO4	SO5	SO6
20	25		25	10	20

Relationship to NQF Outcomes (Out of 100%)				
L7K1	L7S1	L7S2	L7C1	L7C4
20	25	25	10	20

Evaluation	
Assessment Tool	**Weight**
First Exam	20%
Second Exam	20%
Final Exam	50%
Course Work	10%

Date Printed: 2024-10-15