Jordan University of Science and Technology
Faculty of Computer & Information Technology
Software Engineering Department

SE431 Software Security - JNQF Level: 6

Summer Semester 2023-2024

Course Catalog
3 Credit Hours. 3 Credit hours (3 h lectures): Theory and practice of software security, focusing in particular on some common software security risks, including buffer overflows, race conditions, 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	Computer Security: Principles and Practice
Author(s)	William Stallings, Lawrie Brown
Edition	3rd Edition
Short Name	Ref #1
Other Information	

Course References

Short name	Book name	Author(s)	Edition	Other Information
Ref #2	Security in Computing	Charles P. Pfleeger, Shari L. Pfleeger	4th Edition	
Ref #3	Computer Security	Dieter Gollmann	2nd Edition	
Ref #4	Matt Bishop "Introduction to Computer Security"	Addison Wesley	1st Edition	

Class Schedule & Room

Tentative List of Topics Covered		
Weeks	**Topic**	**References**
Weeks 1, 2	Introduction	**Chapter 1** From **Ref #1**
Weeks 3, 4	Access Control	**Chapter 4** From **Ref #1**
Weeks 5, 6, 7	Software Security	**Chapter 11,12** From **Ref #1**
Weeks 8, 9	Intrusion Detection	**Chapter 6** From **Ref #1**
Weeks 10, 11, 12	Malicious Software (Viruses and other Malicious Code)	**Chapter 7** From **Ref #1**
Weeks 3, 4, 5	Cryptography	**Chapter 2,19,20** From **Ref #1**
Week 16	Database Security	

Mapping of Course Outcomes to Program Outcomes and NQF Outcomes	Course Outcome Weight (Out of 100%)	Assessment method
Comprehend basic security terminologies, and specifically the basic goals of software security, that is, confidentiality, integrity and availability. [1C1, 1B1] [1L6K1]	20%	
Use the proper authentication method based on the application being used. And accordingly use the proper access control mechanism. [1C6, 1B6] [1L6C3]	25%	
Distinguish between the different types of malwares and use the proper techniques to protect against them. [1C10, 1B10] [1L6K1]	20%	
Identify and describe different types of widely used encryption algorithms such as DES. AES and RSA and their applications in the real life. [1C9, 1B9] [1L6S1]	20%	
Practice secure programming. [1C3, 1B3] [1L6C2]	5%	
Remediate common web application vulnerabilities and apply defensive application design and coding practices to avoid security vulnerabilities. [1C6, 1B6] [1L6C4]	5%	
Investigate different security protocols. [1C12, 1B12] [1L6C3]	5%	

Relatio																								
SM1p	SM2p	SM3p	EA1p	EA2p	EA3p	EA4p	D1p	D2p	D3p	D4p	D5p	D6p	ET1p	ET2p	ET3p	ET4p	ET5p	ET6p	EP1p	EP2p	EP3p	EP4p	EP5p	EP6p

Relationship to NQF Outcomes (Out of 100%)				
L6K1	L6S1	L6C2	L6C3	L6C4
40	20	5	30	5

Evaluation	
Assessment Tool	**Weight**
Midterm	20%
Project	10%
Final	50%
Assignments and Lab	15%
Quizzes	5%

Policy	
Attendance	Attendance is very important for the course. In accordance with university policy, students missing more than 10% of total classes are subject to failure. Penalties may be assessed without regard to the student's performance. Attendance will be recorded at the beginning or end of each class.
Homework/Lab	Students are expected to keep up with the material as it is presented and submit assignments on time. Students are expected to do their work individually. Any students do the work in teams will be considered an attempt for cheating.
Exams	All exams are closed book.

Date Printed: 2024-07-15