Ministry of Higher Education and
Scientific Research - Iraq
University of Technology
Department of Computer Science
Information System Branch

MODULE DESCRIPTOR FORM

نموذج وصف المادة الدراسية

Module Information
معلومات المادة الدراسية

Module Title	SOFTWARE SECURITY	**Module Delivery**	
Module Type	C	**-Theory Lecture**	
Module Code	SOSE225		
ECTS Credits	4.00		
SWL (hr/sem)	100		
Module Level	2	**Semester of Delivery**	
Administering Department	Computer and cyber security	**College**	Computer science department
Module Leader	Ayad Hazim	**e-mail**	Ayad.h.ibrahim@uotechnology.edu.iq
Module Leader's Acad. Title	Assoc. Prof.Dr.	**Module Leader's Qualification**	PhD.
Module Tutor	None	**e-mail**	None
Peer Reviewer Name		**e-mail**	
Review Committee Approval		**Version Number**	

Relation With Other Modules
العلاقة مع المواد الدراسية الأخرى

Prerequisite module	AUAC215	**Semester**	Two

Co-requisites module	MAC0314	**Semester**	Five

Module Aims, Learning Outcomes and Indicative Contents
أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية

Module Aims أهداف المادة الدراسية	1. Teach student the fundamental of security risk of any software 2. Teach student the possible attack types. 3. Teach student the possibility of threatening in software design. 4. Teach how to build software that
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	**A- Knowledge and Understanding** 1: Qualifying students to explore the importance of software security and possible threaten. 2: Qualifying students to deal with data security background. 3: Qualifying students to identify and solve security issues related to software. **B- Subject-specific skills** 1: Enable students to identify the data security for any software design. 2: Give the means to students for linking data security with designing software 3: Enable students to understand the advantage of building strong and speed software with a complete security requirements.
Indicative Contents المحتويات الإرشادية	1: Clarify some concepts of computer security 2: Clarify the importance of information security in software applications 3: Clarify the importance of employing the security of software designs in software applications

Learning and Teaching Strategies
استراتيجيات التعلم والتعليم

Strategies	Methodological books, resources (internet and library), dialogues reinforced with illustrative examples,Theoretical lectures, practical tasks, using modern devices to present practical ideas to students (data show, electronic board)

Student Workload (SWL)
الحمل الدراسي للطالب

Structured SWL (h/sem) الحمل الدراسي المنتظم للطالب خلال الفصل	64	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	2
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطالب خلال الفصل	36	**Unstructured SWL (h/w)** الحمل الدراسي غير المنتظم للطالب أسبوعيا	

Total SWL (h/sem) الحمل الدراسي الكلي للطالب خلال الفصل	100

Module Evaluation
تقييم المادة الدراسية

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	1	10% (10)	5	LO # 1 and 3
	Practical Seminar(Lab).	2	15% (15)	Continuous	LO # 2 , 4 and 5
Summative assessment	**Midterm Exam**	1 hr	15% (15)	14	LO # 1 to 5
	Final Exam	3hr	60% (60)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)
المنهاج الاسبوعي النظري

	Material Covered
Week 1	**Introduction to Software and System Security Principles**
Week 2	Authentication factors and access rights
Week 3	Confidentiality, Integrity, and Availability
Week 4	1. Isolation 2. Least Privilege 3. Compartmentalization
Week 5	Threat models and bug versus Vulnerability in software
Week 6	**Attack Vectors modules**
Week 7	1. Denial of Service (DoS) 2- Information Leakage
Week 8	1. Confused Deputy 2- Privilege Escalation
Week 9	1. Control-Flow Hijacking 2. Code Injection 3. Code Reuse

Week 10	Redesign software modules
Week 11	**Defense Strategies in software design**
Week 12	1. Software Verification 2. Language-based Security
Week 13	3. Testing software Testing • Manual Testing • Sanitizers • Fuzzing • Symbolic Execution
Week 14	Mitigations • Data Execution Prevention (DEP)/W^X 86 • Address Space Layout Randomization (ASLR) • Stack integrity • Safe Exception Handling (SEH)
Week 15	• Fortify Source • Control-Flow Integrity • Code Pointer Integrity • Sandboxing and Software-based Fault Isolation
Week 16	Final Exam

Delivery Plan (Weekly Lab. Syllabus) **المنهاج الاسبوعي للمختبر**	
Week	
Week 1	
Week 2	
Week 3	
Week 4	
Week 5	
Week 6	
Week 7	
Week 8	
Week 9	
Week 10	

Week 11	
Week 12	
Week 13	

Learning and Teaching Resources مصادر التعلم والتدريس		
	Text	**Available in the Library?**
Required Texts	Cryptography and Network Security Principles and Practice, FifthEdition,William stallings. Software Security Principles, Policies, and Protection, Mathias Payer, July 2021, v0.37	
Recommended Texts		
Websites		

APPENDIX:

GRADING SCHEME مخطط الدرجات				
Group	**Grade**	التقدير	**Marks (%)**	**Definition**
Success Group (50 - 100)	**A -** Excellent	امتياز	90 - 100	Outstanding Performance
	B - Very Good	جيد جدا	80 - 89	Above average with some errors
	C - Good	جيد	70 - 79	Sound work with notable errors
	D - Satisfactory	متوسط	60 - 69	Fair but with major shortcomings
	E - Sufficient	مقبول	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX** – Fail	مقبول بقرار	(45-49)	More work required but credit awarded
	F – Fail	راسب	(0-44)	Considerable amount of work required
Note:				

NB Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.