



Ministry of Higher Education and
Scientific Research - Iraq
University of Diyala
College of Engineering for Artificial
Intelligence Technology
Department of Cybersecurity Engineering



الملحق ٤: وصف المادة الدراسية

MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

Module Information			
معلومات المادة الدراسية			
Module Title	Secure Programming		Module Delivery
Module Type	Core		☒ Theory ☒ Lecture ☐ Lab ☐ Tutorial ☐ Practical ☐ Seminar
Module Code	CSE 211		
ECTS Credits	6		
SWL (hr/sem)	150		
Module Level	2	Semester of Delivery	
Administering Department	Cybersecurity Eng.	College	College of Artificial Intelligence Engineering Technology
Module Leader	Ali N. Albu-Rghaif	e-mail	ali.alburghaif@uodiyala.edu.iq
Module Leader's Acad. Title	Asst. Professor	Module Leader's Qualification	Ph.D.
Module Tutor	Name (if available)	e-mail	E-mail
Peer Reviewer Name		e-mail	
Scientific Committee Approval Date	14/05/2026	Version Number	1.0

Relation with other Modules			
العلاقة مع المواد الدراسية الأخرى			
Prerequisite module	CSE 106	Semester	
Co-requisites module	None	Semester	



**Ministry of Higher Education and
Scientific Research - Iraq
University of Diyala
College of Engineering for Artificial
Intelligence Technology
Department of Cybersecurity Engineering**



Module Aims, Learning Outcomes and Indicative Contents

أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية

Module Objectives أهداف المادة الدراسية	By the end of this module, students will be able to: 1. Introduce students to the principles of secure programming and software security 2. Develop the ability to identify and mitigate common software vulnerabilities 3. Teach secure coding practices across different programming contexts 4. Provide hands-on experience in analyzing and fixing insecure code 5. Introduce basic low-level security concepts (e.g., memory vulnerabilities) 6. Prepare students to integrate security into the software development lifecycle
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	Upon successful completion of this module, students should be able to: 1. Identify common software vulnerabilities and security flaws 2. Apply secure coding techniques to prevent common attacks 3. Analyze and debug insecure code 4. Implement input validation and secure error handling 5. Demonstrate understanding of authentication and access control mechanisms 6. Explain basic cryptographic concepts and apply them appropriately 7. Describe basic memory-related vulnerabilities (e.g., buffer overflow) 8. Use security tools to test and evaluate software security
Indicative Contents المحتويات الإرشادية	• Introduction to Secure Programming • Software Vulnerabilities and Threats • OWASP Top 10 Overview • Input Validation and Output Encoding • Secure Error Handling • Authentication and Authorization • Password Security (Hashing & Salting) • Basics of Cryptography • Secure File Handling • Web Security Basics (XSS, SQL Injection, CSRF) • Introduction to Memory Security (Buffer Overflow – concept level) • Secure APIs and Session Management • Secure Software Development Lifecycle (SSDLC) • Code Review and Security Testing
Learning and Teaching Strategies استراتيجيات التعلم والتعليم	
Strategies	The module will be delivered using a combination of: • Interactive lectures and classroom discussions. • Practical laboratory sessions focused on secure coding practices. • Hands-on vulnerability analysis and debugging exercises. • Demonstrations of common software attacks and mitigation techniques.



**Ministry of Higher Education and
Scientific Research - Iraq
University of Diyala
College of Engineering for Artificial
Intelligence Technology
Department of Cybersecurity Engineering**



	• Individual and group-based secure programming projects. • Code review and peer evaluation activities. • Use of security testing and vulnerability assessment tools. • Continuous assessment through quizzes, assignments, labs, and project presentations.
--	---

Student Workload (SWL) الحمل الدراسي للطلاب محسوب ل ١٥ اسبوعا			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطلاب خلال الفصل	78	Structured SWL (h/w) الحمل الدراسي المنتظم للطلاب أسبوعيا	5.2
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطلاب خلال الفصل	72	Unstructured SWL (h/w) الحمل الدراسي غير المنتظم للطلاب أسبوعيا	4.8
Total SWL (h/sem) الحمل الدراسي الكلي للطلاب خلال الفصل	150		

Module Evaluation تقييم المادة الدراسية					
		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	Quizzes	2	10% (5)	6 and 14	LO #1 to #9
	Assignments	2	10% (5)	4, 7 and 10	LO #1 - #8
	Class Work	2	10% (5)		
	Projects / Lab.	1	10%		
	Report				
Summative assessment	Midterm Exam	1 hr	10% (10)	9	LO #1 to #6
	Final Exam	3 hr	50% (50)	16	All
Total assessment			100% (100 Marks)		



**Ministry of Higher Education and
Scientific Research - Iraq
University of Diyala
College of Engineering for Artificial
Intelligence Technology
Department of Cybersecurity Engineering**



Delivery Plan (Weekly Syllabus)

المنهاج الاسبوعي النظري

	Material Covered
Week 1	Introduction to Secure Programming & Secure Design Principles - Importance of secure coding - Overview of threats and attacks
Week 2	Software Vulnerabilities - Types of vulnerabilities - OWASP Top 10 overview
Week 3	Injection Attacks - SQL Injection - Command Injection - Prevention techniques
Week 4	Cross-Site Scripting (XSS) - Types of XSS - Input/output handling
Week 5	CSRF & Session Attacks - CSRF attacks - Session hijacking basics
Week 6	Input Validation & Data Sanitization - Validation techniques - Encoding and sanitization
Week 7	Authentication & Authorization - Access control models - Secure login systems
Week 8	Password Security - Hashing & Salting - Password policies
Week 9	Midterm Review and Exam
Week 10	Basics of Cryptography - Symmetric vs Asymmetric encryption - Hash functions
Week 11	Secure File Handling - File upload vulnerabilities - Path traversal
Week 12	Introduction to Memory Security - Buffer overflow concept - Stack basics (simplified)
Week 13	Secure APIs & Web Security - API security basics - HTTPS & secure communication



**Ministry of Higher Education and
Scientific Research - Iraq
University of Diyala
College of Engineering for Artificial
Intelligence Technology
Department of Cybersecurity Engineering**



Week 14	Secure SDLC - Secure design principles - Threat modeling basics
Week 15	Code Review & Security Testing - Static and dynamic analysis - Tools overview
Week 16	Preparatory week before the final Exam

Delivery Plan (Weekly Lab. Syllabus) المنهاج الاسبوعي للمختبر	
	Material Covered
Week 1	Laboratory environment may utilize Linux-based systems and cross-platform development tools for secure programming exercises. Lab setup (Linux / tools installation) Introduction to secure coding environment
Week 2	Identifying vulnerabilities in simple code Basic OWASP examples
Week 3	SQL Injection demo and prevention Secure database queries
Week 4	XSS attack simulation Input/output sanitization
Week 5	CSRF demonstration Session management basics
Week 6	Implement input validation functions Data sanitization practice
Week 7	Build a simple login system with access control
Week 8	Password hashing using secure algorithms
Week 9	Basic cryptography implementation (encryption & hashing)
Week 10	Secure file upload implementation Prevent path traversal
Week 11	Simple buffer overflow demonstration (controlled environment)
Week 12	Secure API requests (tokens, headers)
Week 13	Threat modeling exercise (mini case study)
Week 14	Code review session using tools Vulnerability scanning
Week 15	Final project demo (secure application)



**Ministry of Higher Education and
Scientific Research - Iraq
University of Diyala
College of Engineering for Artificial
Intelligence Technology
Department of Cybersecurity Engineering**



Learning and Teaching Resources مصادر التعلم والتدريس		
	Text	Available in the Library?
Required Texts	- Secure Coding in C and C++ by Robert C. Seacord - Writing Secure Code by Michael Howard and David LeBlanc - Software Security: Building Security In by Gary McGraw	No
Recommended Texts	- The Web Application Hacker's Handbook by Dafydd Stuttard and Marcus Pinto - Secure Programming Cookbook for C and C++ by John Viega and Matt Messier - Cryptography and Network Security by William Stallings	No
Websites	OWASP Foundation CWE – Common Weakness Enumeration NIST Computer Security Resource Center PortSwigger Web Security Academy Mozilla Web Security Guidelines SANS Secure Coding Resources	

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	راسب (قيد المعالجة)	(45-49)	More work required but credit awarded
	F – Fail	راسب	(0-44)	Considerable amount of work required

Note: Marks 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.



**Ministry of Higher Education and
Scientific Research - Iraq
University of Diyala
College of Engineering for Artificial
Intelligence Technology
Department of Cybersecurity Engineering**

