نموذج وصف المقرر الدراسي

معلومات المقرر الدراسية				
اسم المقرر	أساسيات الأمن السيبراني			أسلوب التدريس
نوع المقرر	رئيسة			
رمز المقرر	**IT3202**			☒ محاضرة ☒ عملي
عدد الوحدات	**6**			
عدد ساعات المقرر	**150**			
مستوى المقرر الدراسي	3	الفصل الدراسي		2
القسم الأكاديمي	تكنولوجيا المعلومات	الكلية		كلية العلوم
مسؤول المادة	أ.م.د احسان احمد محمد لهمود	الايميل		ahssan.ahsan@gmail.com
اللقب العلمي	مدرس	الشهادة الاكاديمية		دكتوراه
مدرس المادة	أ.م.د احسان احمد محمد لهمود	الايميل		ahssan.ahsan@gmail.com
اسم مراجع المقرر الدراسي	م.د علي كريم عبدالرحيم	الايميل		alialmujab@uowa.edu.iq
تاريخ موافقة اللجنة العلمية	2025-2026	اصدار		V1

العلاقة مع المقررات الدراسية الاخرى			
المتطلب السابق للمادة	-	الفصل الدراسي	-
المتطلبات المصاحبة للمادة	-	الفصل الدراسي	-

مصادقة رئيس القسم

مصادقة السيد عميد الكلية المحترم

أهداف المادة، ومخرجات التعلم، والمحتوى الإرشادي	
هدف المادة الدراسية	1. تزويد الطلبة بفهم راسخ لمفاهيم قواعد البيانات ومبادئها وأفضل الممارسات المعتمدة فيها. 2. تعريف الطلبة بأسس تصميم قواعد البيانات وتنفيذها وإدارتها. 3. تغطية موضوعات مثل نمذجة البيانات، والتطبيع(Normalization) ، وتحسين الاستعلامات (Query Optimization). 4. تنمية المهارات العملية في استخدام أنظمة إدارة قواعد البيانات ولغات الاستعلام. 5. تنمية مهارات التفكير النقدي وحل المشكلات في سياق تصميم وإدارة قواعد البيانات. 6. إعداد الطلبة لتطبيق معارفهم في بيئات وسيناريوهات واقعية. 7. تمكين الطلبة من الإسهام في تطوير حلول فعّالة لقواعد البيانات ضمن قطاع تقنية المعلومات.
مخرجات تعلم المادة الدراسية	1. فهم المفاهيم والمبادئ الأساسية لقواعد البيانات، بما في ذلك نماذج البيانات، المخططات (Schemas)، والتطبيع.(Normalization) 2. إظهار الكفاءة في تصميم وتنفيذ وإدارة قواعد البيانات باستخدام نظام إدارة قواعد البيانات (DBMS). 3. تطبيق تقنيات نمذجة البيانات لتطوير تصميمات منطقية وفيزيائية لقواعد البيانات تلبي المتطلبات المحددة. 4. إنشاء وتنفيذ استعلامات SQL معقدة لاسترجاع البيانات وتحديثها والتعامل معها داخل قاعدة البيانات. 5. تقييم وتحسين أداء الاستعلامات من خلال استخدام الفهارس(Indexing) ، وضبط الاستعلامات(Query Tuning) ، وتقنيات التحسين الأخرى. 6. تنفيذ وفرض قيود تكامل البيانات، بما في ذلك علاقات الكيانات، التكامل المرجعي، وقواعد التحقق من صحة البيانات. 7. استخدام إجراءات أمان مناسبة لحماية البيانات وضمان سرية وسلامة وتوافر قاعدة البيانات. 8. الاستفادة من إجراءات النسخ الاحتياطي والاسترجاع لحماية البيانات وإعادة قاعدة البيانات في حالات الفشل أو الكوارث.
المحتوى الإرشادي	

	العناوين			
		الوصف		الوزن
	1	وجهات نظر الأمن السيبراني وتأثيرها	5.00	5
	2	أهداف وآليات سياسات الأمن السيبراني	5.00	5
	3	خدمات الأمن، الآليات، والتدابير المضادة	10.00	5
	4	الثغرات، التهديدات والمخاطر	10.00	10
	5	المعلومات الشخصية	5.00	10
	6	الهندسة الاجتماعية	5.00	–
	7	الهجمات السيبرانية والكشف عنها	5.00	15
	8	الهجمات السيبرانية وأدوات الحماية	10.00	–
	9	التصيّد الاحتيالي (Phishing) ونواقل الهجوم والاستغلال المرتبطة	5.00	–
	10	المبادئ التسعة للأمن السيبراني	5.00	–

استراتيجيات التعليم والتعلم	
استراتيجيات	**استراتيجيات نظرة عامة على المقرر** تعد الأمن السيبراني ليس مجرد مشكلة تقنية، بل هي أيضًا مشكلة بشرية، حيث يلعب الأفراد دورًا محوريًا في المخاطر المرتبطة بالتهديدات السيبرانية، وكذلك في التخفيف من هذه المخاطر. يوفر هذا المقرر رؤى واستراتيجيات ومهارات للتعامل مع نقاط الضعف في التحكم المرتبطة بسلوك الأفراد في المنظمة، والتي قد تعرض الأعمال للتهديدات السيبرانية. • من المهم أيضًا تقدير أهمية الأفراد، والقوانين، والأخلاقيات في إدارة برامج الأمن السيبراني داخل المؤسسات. • لكي يتمكن الطلاب من إدارة وحماية أصول المعلومات في المؤسسات بفعالية، يجب عليهم تطوير المعرفة والمهارات اللازمة للتخطيط الأمني، وتطوير، وتنفيذ، وتقييم سياسات وبرامج الأمن. • يوفر هذا المقرر للطلاب المعرفة والمهارات والعمليات اللازمة للاستجابة المناسبة والتعافي عند اكتشاف حادثة أمنية سيبرانية من خلال العديد من المحاضرات. • يتم تزويد الطلاب بمبادئ الأمن السيبراني، مع شرح كيفية التخطيط، والكشف، والاستجابة، والتعافي من التهديدات السيبرانية الحالية والناشئة. • يعرّف الطلاب على كيفية اكتشاف وإصلاح الثغرات، وتقنيات التشفير، وكشف التسلل، وإدارة المخاطر السيبرانية. • يتم استعراض تطبيق الممارسات العملية المناسبة التي تدعم موقفًا قويًا في الأمن السيبراني في مجالات تطوير البرمجيات، وإدارة الأنظمة، ومهن نظم المعلومات، من خلال المحاضرات، والتمارين العملية في المختبرات، والواجبات حول مواضيع محددة، والمشاريع الصغيرة.

حمل عمل الطالب			
الساعات المجدولة (ساعات/فصل دراسي)	60	الساعات المجدولة (ساعات/أسبوع)	4
الساعات غير المجدولة (ساعات/فصل دراسي)	87	الساعات غير مجدولة (ساعات/أسبوع)	6
الإجمالي (ساعات/فصل دراسي)	147 + 3 نهائي = 150		

تقييم المقرر الدراسي					
		الوقت/العدد	الوزن (الدرجات)	الأسابيع	مخرجات التعلم
التقويم التكويني	اختبارات	4	8% (8)	3,6,10,13	
	واجبات داخل الكلية	6	12% (12)	3,5,6,8,10,12	
	مشروع	1	10% (10)	يبدا بالأسبوع 4 وينتهي بالأسبوع 14	
	المختبرات	5	10% (10)	7,13	
التقييم النهائي	امتحان المد	2hr	10% (10)	7	
	امتحان النهائي	3hr	50% (50)	16	
إجمالي التقييم			100% (100)		

خطة التدريس (المنهج الأسبوعي)		
	المنهج الدراسي	
الأسبوع 1	**وجهات نظر وتأثيرات الأمن السيبراني** • فهم المشكلات الصعبة في الأمن السيبراني التي تجعل التطبيق تحديًا مستمرًا. • وصف كيفية تسبب حدث سيبراني مهم في زيادة التركيز المؤسسي على الأمن السيبراني. • سرد قصة حول تقدم كبير في مجال الأمن السيبراني.	2
الأسبوع 2	**وجهات نظر وتأثيرات الأمن السيبراني – تابع** • تقييم انتهاك السرية أو النزاهة أو التوافر (CIA) للمعلومات وكيفية تأثير ذلك على الثقة بالمعلومات • مقارنة وتقييم طرق/تطبيقات العملات الرقمية المختلفة.	2
الأسبوع 3	**أهداف وآليات السياسات** • التعرف على تركيز المؤسسة على الالتزام بالمعايير مقابل أفضل الممارسات مقابل أحدث التقنيات. • الوعي بتعدد تعريفات كلمة "سياسة" في سياق الأمن السيبراني. • النظر في إشعار الثغرات والمشكلات المرتبطة بإصلاحها أو عدم إصلاحها والكشف عنها أو عدم الكشف عنها.	2
الأسبوع 4	**أهداف وآليات السياسات – تابع** • مقارنة تأثير الاعتماد على التصميم المفتوح مقابل سرية التصميم للأمن. • توضيح سبب كون الأمن السيبراني ضرورة مجتمعية.	2
الأسبوع 5	**خدمات الأمن، الآليات، والتدابير المضادة** • تحليل موازنة الخصائص الأمنية الأساسية (السرية، النزاهة، والتوافر). • فهم مفاهيم المخاطر، والتهديدات، والثغرات، ومسارات الهجوم. • توثيق مثال على "التدابير المضادة" للتهديدات المحددة. • إعداد قائمة بالأدوات والقدرات لتحديد المخاطر السيبرانية بشكل مستمر. • توضيح مفهوم إدارة الهوية وأهميته.	2
الأسبوع 6	**خدمات الأمن، الآليات، والتدابير المضادة – تابع** • فهم مفاهيم المصادقة، التفويض، والتحكم في الوصول. • الدفاع عن فوائد المصادقة متعددة العوامل. • شرح المصادقة، التفويض، والتحكم في الوصول. • توضيح فوائد المصادقة الثنائية، بما في ذلك استخدام القياسات الحيوية. • تعريف قائمة السماح للتطبيقات.(Application Whitelisting) • تحديد التكاليف والمفاضلات المرتبطة بتنفيذ الأمن في المنتجات.	2
الأسبوع 7	**مراجعة امتحان منتصف الفصل**	2
الأسبوع 8	**الثغرات، التهديدات والمخاطر** • توضيح الفروق بين الثغرات والتهديدات والمخاطر. • وصف كيفية احتواء الثغرات بواسطة آليات الأمن. • استخدام إطار إدارة المخاطر. • استخدام أدوات اختبار الاختراق لتحديد الثغرات. • توضيح فوائد الدفاع المتعمق (Defense in Depth) باستخدام طبقات متعددة من الحماية. • وصف كيفية نشوء المشكلات الأمنية عند حدود المكونات.	2
الأسبوع 9	**الثغرات، التهديدات والمخاطر – تابع** • استخدام قاعدة البيانات الوطنية للثغرات لتحديد وجود ثغرات في البرمجيات المثبتة على الخوادم أو مكونات الشبكة. • التعرف على الثغرات والتهديدات والمخاطر الخاصة بالبنية التحتية للشبكة، الخوادم السحابية، أجهزة الكمبيوتر المكتبية، والأجهزة المحمولة. • استخدام هجوم تجاوز السعة (Buffer Overflow) على خادم.	2

	• استخدام هجوم البرمجة عبر المواقع (Cross-Site Scripting) على خادم لا يقوم بتنقية مدخلات المستخدم بشكل صحيح.	
الأسبوع 10	**المعلومات الشخصية** • فهم المصطلحات: المعلومات الشخصية، المعلومات القابلة للتحديد، إزالة التحديد، التعمية، الاسم المستعار، الإخفاء والكشف. • وصف كيفية تطبيق مبادئ المعلومات العادلة (Fair Information Practices) على المعلومات الشخصية وجمعها واستخدامها عبر الإنترنت. • تصنيف عدة فئات من المعلومات الشخصية وفقًا لمستوى الخصوصية ومخاطر الإفصاح.	2
الأسبوع 11	**المعلومات الشخصية – تابع** • مقارنة السياسات الخاصة بجمع ومعالجة وتخزين ومشاركة والتخلص من المعلومات الشخصية. • توضيح دور وحدود التشفير في حماية المعلومات الشخصية. • فهم السياسات والتقنيات لعزل البيانات الشخصية عن بيانات المؤسسة. • تحليل طرق التحكم في الوصول إلى المعلومات الشخصية.	2
الأسبوع 12	**الهجمات السيبرانية والكشف عنها** • تعريف أدوار آليات الوقاية، الردع، والكشف. • التعرف على تخمين كلمات المرور، فحص المنافذ، هجمات SQL Injection وغيرها في ملفات السجل. • مناقشة دور وحدود تقنيات مكافحة الفيروسات القائمة على التوقيع والسلوك.	2
الأسبوع 13	**الهجمات السيبرانية والكشف عنها – تابع** • شرح فرقين بين أنظمة كشف التسلل على المضيف والشبكة. • إنشاء ثلاثة قواعد لنظام كشف التسلل الشبكي للحماية من هجمات محددة. • مناقشة استخدام الخداع بواسطة البرمجيات الضارة لتجنب آليات الأمان.	2
الأسبوع 14	**الهجمات السيبرانية وأدوات الأمان** • شرح مفاهيم الاختراق والتصيد الاحتيالي. • التعرف على هجمات الحرمان من الخدمة (DoS) والبريد المزعج .(Spam Email) • أنواع أدوات الأمان ونصائح السلامة ضد الجرائم الإلكترونية. • اتباع تعليمات مبادئ الأمن السيبراني.	2
الأسبوع 15	**تقييم عبء الطالب على المقرر**	2
الأسبوع 16	**التحضير للامتحان النهائي**	3

خطة التدريس (المنهج الأسبوعي)

	المنهج الدراسي	
الأسبوع 1	• إعداد بيئة مختبر الأمن السيبراني. • مقدمة في مفاهيم الأمن السيبراني. • توضيح الفرق بين الخصوصية وحقوق النشر ومفهوم الأمن. • تثبيت الأجهزة الافتراضية وبعض أدوات الأمن لاستخدامها في مختبر الاختراق.	2
الأسبوع 2	• التعرف على كيفية جمع المخترقين للمعلومات الحساسة مثل بيانات بطاقات الائتمان أو كلمات المرور دون علم الضحية باستخدام أسلوب Harvesting Credential.	2
الأسبوع 3	• التعرف على كيفية عمل هجوم حجب الخدمة (DoS). • اكتشاف الثغرات في أجهزة الاختبار الخاصة بالحقن.	2

الأسبوع 4	• تثبيت أدوات أمنية لاستكمال مختبر 3. • تثبيت أنظمة اختبار للحقن.	2
الأسبوع 5	• تثبيت بيئة اختبار SQL Injection. • التعرف على كيفية تلاعب المخترقين بالمعلومات. • دراسة التدابير المضادة.	2
الأسبوع 6	• تثبيت الجهاز الافتراضي Metasploitable2 لاختبار الثغرات.	2
الأسبوع 7	• اختبار عملي أول للمختبر مع التقييم.	2
الأسبوع 8	• التعرف على كيفية تنفيذ هجوم تصعيد الصلاحيات. • استغلال Injection SQL لتنفيذ تصعيد صلاحيات. • تثبيت نظام Kali Linux. • إعداد مختبر Pentastar: من SQL Injection إلى Shell.	2
الأسبوع 9	• تثبيت XAMPP على Kali. • تثبيت OWASP Mutillidae II. • استغلال ضعف التحكم في الوصول.	2
الأسبوع 10	• تعلم استخدام أداة Burp Suite لاعتراض طلبات المستخدم. • استخدام Burp Suite في اختبار تطبيقات الويب.	2
الأسبوع 11	• استغلال ثغرة التحكم في الوصول لتسجيل الدخول كمستخدم آخر. • فهم مخاطر ضعف فرض القيود على المستخدمين المصادق عليهم. **هجوم صفحات التصيد الاحتيالي:** • استخدام صفحات أصلية لخداع الضحية. • إنشاء صفحة تصيد باستخدام أداة Hidden Eye. • الحصول على بيانات اعتماد تجريبية لأغراض تعليمية.	2
الأسبوع 12	**هجوم الرجل في الوسط (MITM)** • التقاط بيانات تسجيل الدخول FTP. • استخدام أداة Ettercap وتشغيل Kali Linux في وضع Mode Bridge.	2
الأسبوع 13	• اختبار عملي ثانٍ للمختبر مع التقييم.	2
الأسبوع 14	**هجوم كسر كلمات المرور** • إنشاء قائمة كلمات مرور مخصصة باستخدام أداة Crunch.	2
الأسبوع 15	• تنفيذ مشروع الأمن السيبراني مع مناقشة لكل طالب.	2

المصادر التعليمية والتدريسية		
	النص	متوفر في المكتبة؟
الكتب الأساسية / المطلوبة	1. أنظمة قواعد البيانات الموزعة – فيرا غوبيل 2. أنظمة إدارة قواعد البيانات الموزعة: نهج عملي	نعم
الكتب الموصي بها	1. أنظمة قواعد البيانات الموزعة 2. الأنظمة الموزعة 3. مبادئ أنظمة قواعد البيانات الموزعة 4. قاعدة البيانات الموزعة 5. أنظمة الإدارة	
المواقع الإلكترونية	https://www.tutorialspoint.com/distributed_dbms/distributed_dbms_databases.htm What is a distributed database? | Definition from TechTarget Principles of Distributed Database Systems | SpringerLink	

مخطط الدرجات				
المجموعة	الدرجة	التقدير	التقدير%	التقدير
مجموعة النجاح (100 - 50)	A - ممتاز	امتياز	90 - 100	أداء ممتاز
	B-جيد جداً	جيد جدا	80 - 89	فوق المتوسط مع بعض الأخطاء
	C-جيد	جيد	70 - 79	عمل جيد مع أخطاء ملحوظة
	D- مقبول	متوسط	60 - 69	مقبول لكن مع نقائص كبيرة
	E - كافٍ / مرضٍ	مقبول	50 - 59	العمل يلبي الحد الأدنى من المعايير
مجموعة الرسوب (49 - 0)	FX-راسب (قيد المعالجة)	راسب (قيد المعالجة)	(45-49)	يتطلب مزيدًا من العمل ولكن يُمنح الطالب الدرجة
	F-راسب	راسب	(0-44)	يتطلب قدرًا كبيرًا من العمل
ملاحظة:				

سيتم تقريب العلامات العشرية التي تزيد أو تقل عن 0.5 إلى العلامة الكاملة الأعلى أو الأدنى (على سبيل المثال، العلامة 54.5 سيتم تقريبها إلى 55، بينما العلامة 54.4 سيتم تقريبها إلى 54). تطبق الجامعة سياسة عدم قبول حالات الرسوب القريبة من النجاح، لذا فإن التعديل الوحيد للدرجات الممنوحة من قبل المصحح/المصححين الأصليين سيكون التقريب التلقائي الموضح أعلاه فقط.