BAN CƠ YẾU CHÍNH PHỦ

HỌC VIỆN KỸ THUẬT MẬT MÃ

TRẦN THỊ LƯỢNG

NGÂN HÀNG CÂU HỎI THI TỰ LUẬN CẬP NHẬT

AN TOÀN CƠ SỞ DỮ LIỆU

Hà Nội, 2023

PHẦN I. TỔNG HỢP CÁC NỘI DUNG MÔN HỌC

Môn học: An toàn toàn CSDL

Khoa: An toàn thông tin

Các chương trình đào tạo có sử dụng môn học:

P1: ĐH Chính quy An toàn thông tin

Các phần nội dung môn học trong các chương trình đào tạo:

TT	Phần nội dung	P1
1	Tổng quan về an toàn cơ sở dữ liệu	☑
2	Mô hình an toàn cơ sở dữ liệu	☑
3	An toàn trong các DBMS và ứng dụng mật mã trong an toàn CSDL	☑
4	An toàn trong CSDL thống kê	☑
5	Kiểm toán CSDL	☑
6	Phát hiện xâm nhập cho CSDL	☑

PHẦN II. TRÍCH LƯỢC ĐỀ CƯƠNG CHI TIẾT

1. Thông tin chung

Tên học phần	**An toàn toàn CSDL**
Tên tiếng Anh	Database Security
Số tín chỉ	2
Số giờ học ở lớp	36 (24 LT, 12 BT)
Số giờ tự học ở nhà	72
Học phần học trước	

2. Mục tiêu học phần

2.1. Mục tiêu chung

Học phần này cung cấp kiến thức tổng quan về an toàn cơ sở dữ liệu, kiến thức về các mô hình và chính sách an toàn cơ sở dữ liệu, kiến thức và các cơ chế an toàn cơ bản trong các DBMS, kiến thức cơ bản về an toàn cơ sở dữ liệu thống kê, kiến thức về các cơ chế kiểm toán cho CSDL.

2.2. Mục tiêu cụ thể

Mục tiêu	Mô tả	Chuẩn đầu ra CTĐT
M1	Trình bày được kiến thức tổng quan về an toàn cơ sở dữ liệu	
M2	Trình bày và triển khai được các mô hình và chính sách an toàn cơ sở dữ liệu trên các hệ quản trị	
M3	Trình bày được các phương pháp và cơ chế mã hóa CSDL	
M4	Trình bày được đặc điểm, các dạng biểu diễn của CSDL thống kê. Trình bày được được các dạng tấn công suy diễn lên cơ sở dữ liệu thống kê	
M5	Trình bày được vai trò và các cơ chế của kiểm toán cho CSDL	
M6	Triển khai được các cơ chế an toàn cơ bản trong các DBMS như: xác thực, cấp quyền, kiểm toán, mã hóa dữ liệu (SQL Server, Oracle)	
M7	Trình bày được mô hình, các phương pháp và công cụ phát hiện xâm nhập CSDL	
M8	Vận dụng các phương pháp tấn công suy diễn để tấn công lên một CSDL thống kê cụ thể	
M9	Có kỹ năng làm việc nhóm và thuyết trình	
M10	Có kỹ năng đọc hiểu các tài liệu bằng tiếng Anh liên quan đến học phần	
M11	Có thái độ tích cực, chủ động trong học tập	

3. Mô tả học phần

Học phần này trước hết giới thiệu tổng quan về an toàn CSDL (một số khái niệm cơ bản, các hiểm họa và tấn công đối với CSDL, các yêu cầu bảo vệ CSDL). Tiếp đó, học phần trình bày về các mô hình và chính sách an toàn (các mô hình an toàn bắt buộc, mô hình an toàn tùy ý, mô hình an toàn đa mức, v.v). Phần tiếp theo trình bày về an toàn trong các hệ quản trị CSDL (Thiết kế các DBMS an toàn, đảm bảo an toàn CSDL bằng mật mã, các cơ chế an toàn trong Oracle). Sau đó, học phần trình bày về an toàn trong CSDL thống kê (Các khái niệm cơ bản, các đặc trưng của CSDL thống kê, các kiểu tấn công suy diễn vào CSDL thống kê, các kỹ thuật chống tấn công suy diễn, so sánh các kỹ thuật chống suy diễn). Cuối cùng học phần trình bày về Kiểm toán cho CSDL (tổng quan về kiểm toán, các loại kiểm toán, các kiến trúc kiểm toán, kiểm toán trong Oracle).

4. Nội dung học phần

Chương 1 Tổng quan về an toàn cơ sở dữ liệu

1.1. Giới thiệu

1.2. Một số khái niệm cơ bản

1.2.1. Hệ cơ sở dữ liệu

1.2.2. Thiết kế cơ sở dữ liệu

1.2.3. Các mức mô tả dữ liệu

1.2.4. Ngôn ngữ SQL

1.3. Các hiểm hoạ và tấn công đối với cơ sở dữ liệu

1.4. Các yêu cầu bảo vệ cơ sở dữ liệu

1.4.1. Bảo vệ chống truy nhập trái phép

1.4.2. Bảo vệ chống suy diễn

1.4.3. Bảo vệ toàn vẹn cơ sở dữ liệu

1.4.4. Khả năng lưu vết và kiểm tra

1.4.5. Xác thực người dùng

1.4.6. Quản lý và bảo vệ dữ liệu nhạy cảm

1.4.7. Bảo vệ nhiều mức

1.4.8. Sự hạn chế

1.5. Giới thiệu về một số dạng CSDL phổ biến khác SQL

1.5.1. NoSQL

1.5.2. NewSQL

1.5.3. SQL Lite

1.5.4. Realtime Database

1.6. Giới thiệu một số hệ quản trị CSDL thông dụng

1.6.1. Các hệ quản trị SQL thông dụng

1.6.2. Các hệ quản trị NoSQL thông dụng

1.6.3. Các hệ quản trị NewSQL thông dụng

1.7. Câu hỏi ôn tập

Chương 2. Mô hình an toàn cơ sở dữ liệu

2.1. Giới thiệu

2.2. Các mô hình an toàn cơ sở dữ liệu

2.2.1. Kiểm soát truy nhập trong các hệ thống hiện tại

2.2.2. Các mô hình an toàn tùy ý

2.2.3. Các mô hình an toàn bắt buộc

2.2.4 Các mô hình an toàn khác

2.3. Giới thiệu về cơ chế kiểm soát phụ thuộc dữ liệu VPD trong Oracle

2.3.1. Giới thiệu về VPD

2.3.2. Các thành phần của chính sách VPD

2.3.3. Cấu hình một chính sách VPD

2.4. Giới thiệu về kiểm soát bắt buộc OLS trong Oracle

2.4.1 Giới thiệu về OLS

2.4.2. Nhãn dữ liệu và nhãn người dùng

2.4.3. Tạo một chính sách OLS

2.4.4. Sử dụng VPD để thi hành chính sách OLS

2.5. Câu hỏi ôn tập

Chương 3. An toàn trong các DBMS và ứng dụng mật mã trong an toàn CSDL

3.1. An toàn trong các DBMS

3.1.1. Giới thiệu

3.1.2. Các kiến trúc DBMS an toàn

3.1.3. Các vấn đề an toàn chung trong DBMS

3.2. Ứng dụng mật mã trong an toàn cơ sở dữ liệu

3.2.1. Tổng quan về đảm bảo an toàn CSDL bằng mật mã

3.2.2. Mã hóa CSDL trong các DBMS

3.2.3. Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

3.3. Câu hỏi ôn tập.

Chương 4. An toàn trong cơ sở dữ liệu thống kê

4.1. Giới thiệu

4.1.1. Dạng biểu diễn của cơ sở dữ liệu thống kê

4.1.2. Các cơ sở dữ liệu thống kê trong thực tế

4.1.3. Vấn đề bảo vệ cơ sở dữ liệu thống kê

4.2. Các đặc trưng của cơ sở dữ liệu thống kê

4.3. Các khái niệm cơ bản

4.4. Các tấn công suy diễn vào cơ sở dữ liệu thống kê

4.5. Các kỹ thuật chống tấn công suy diễn

4.5.1. Các kỹ thuật khái niệm

4.5.2. Các kỹ thuật hạn chế

4.5.3. Các kỹ thuật gây nhiễu

4.6. So sánh các kỹ thuật chống tấn công suy diễn

4.7. Câu hỏi ôn tập

Chương 5. Kiểm toán CSDL

5.1. Tổng quan về kiểm toán

5.1.1. Các định nghĩa

5.1.2. Vai trò của kiểm toán

5.2. Các loại kiểm toán

5.2.1. Kiểm toán đăng nhập CSDL

5.2.2. Kiểm toán nguồn sử dụng CSDL

5.2.3. Kiểm toán việc sử dụng CSDL ngoài giờ làm việc

5.2.4. Kiểm toán câu lệnh DDL

5.2.5. Kiểm toán câu lệnh DML

5.2.6. Kiểm toán lỗi CSDL

5.2.7. Kiểm toán các thay đổi với nguồn của các thủ tục và trigger

5.3. Các kiến trúc kiểm toán

5.3.1. Các kiến trúc hệ thống kiểm toán bên ngoài

5.3.2. Lưu trữ thông tin kiểm toán

5.3.3. Đảm bảo an toàn thông tin kiểm toán

5.3.4. Kiểm tra hệ thống kiểm toán

5.4. Kiểm toán trong Oracle

5.4.1. Kiểm toán câu lệnh

5.4.2. Kiểm toán đặc quyền

5.4.3. Kiểm toán đối tượng lược đồ

5.4.4. Kiểm toán mịn

5.5. Câu hỏi ôn tập

Chương 6. Phát hiện xâm nhập cho CSDL

6.1. Giới thiệu về phát hiện xâm nhập CSDL

6.2. Mô hình kiến trúc hệ thống phát hiện xâm nhập CSDL

6.3. Giới thiệu một số phương pháp phát hiện xâm nhập CSDL

6.4. Phát hiện xâm nhập bên trong dựa trên hành vi

6.5. Giới thiệu một số công cụ phát hiện xâm nhập CSDL

6.6. Câu hỏi ôn tập

PHẦN III. PHÂN RÃ CHUẨN ĐẦU RA HỌC PHẦN

1. Các chuẩn đầu ra được đánh giá

TT	Ký hiệu	Chuẩn đầu ra
1	CLO1	Trình bày được kiến thức tổng quan về an toàn cơ sở dữ liệu; các mô hình và chính sách an toàn; các phương pháp và cơ chế mã hóa CSDL; đặc điểm, các dạng biểu diễn, các tấn công lên CSDL thống kê; vai trò và các cơ chế của kiểm toán cho CSDL; mô hình, các phương pháp và công cụ phát hiện xâm nhập CSDL.
2	CLO2	Phân tích được các mô hình và chính sách an toàn CSDL
3	CLO3	Vận dụng các phương pháp tấn công suy diễn để tấn công lên một CSDL thống kê cụ thể; Vận dụng kiến thức về thiết kế hệ quản trị CSDL an toàn để bảo vệ một CSDL cụ thể.

PHẦN IV. MA TRẬN ĐỀ THI

1. Chương trình ĐH Chính quy An toàn thông tin (P1)

Tổng số câu hỏi: 3 câu. Thời gian làm bài: 90 phút.

Tài liệu được phép sử dụng: Không

Cấu trúc đề thi:

Ký hiệu	Nhóm câu hỏi	CLO	Cấp độ	Số lượng	Hệ số điểm
1	Trình bày được kiến thức tổng quan về an toàn cơ sở dữ liệu; các mô hình và chính sách an toàn; các phương pháp và cơ chế mã hóa CSDL; đặc điểm, các dạng biểu diễn, các tấn công lên CSDL thống kê; vai trò và các cơ chế của kiểm toán cho CSDL; mô hình, các phương pháp và công cụ phát hiện xâm nhập CSDL.	CLO1	NB	1	3
2	Phân tích được các mô hình và chính sách an toàn CSDL	CLO2	TH	1	3
3	Vận dụng các phương pháp tấn công suy diễn để tấn công lên một CSDL thống kê cụ thể; Vận dụng kiến thức về thiết kế hệ quản trị CSDL an toàn để bảo vệ một CSDL cụ thể.	CLO3	VD	1	4
	Tổng số câu hỏi trong đề thi			**3**	**10**