HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA CÔNG NGHỆ THÔNG TIN 1
*****

ĐỀ CƯƠNG MÔN HỌC
(Phương pháp đào tạo theo tín chỉ)

TÊN HỌC PHẦN: AN TOÀN ỨNG DỤNG WEB VÀ CƠ SỞ DỮ LIỆU

Mã học phần: INT14105
(3 tín chỉ)

Biên soạn
HOÀNG XUÂN DẬU

Hà Nội - 2021

ĐỀ CƯƠNG HỌC PHẦN: AN TOÀN ỨNG DỤNG WEB

Khoa: Công nghệ thông tin 1 **Bộ môn**: An toàn thông tin

1.Thông tin về giảng viên

(Những Giảng viên có thể tham gia giảng dạy được môn học,hoặc Bộ môn có kế hoạch để Giảng viên chuẩn bị giảng dạy được môn học)

1.1. Giảng viên 1:

Họ và tên: ……Hoàng Xuân Dậu ……

Chức danh, học hàm, học vị: ……Tiến sỹ, Giảng viên ……..

Địa điểm làm việc: Bộ môn An toàn thông tin, Khoa CNTT1,
Học viện Công nghệ Bưu chính Viễn thông

Địa chỉ liên hệ: Bộ môn An toàn thông tin, Khoa CNTT1, Cơ sở đào tạo Hà đông
Học viện Công nghệ Bưu chính Viễn thông

Điện thoại: … 0904 534 390 …… Email: dauhx@ptit.edu.vn

Các hướng nghiên cứu chính: An toàn và bảo mật thông tin, học máy, khai phá dữ liệu và các hệ thống nhúng.

Thông tin về trợ giảng (nếu có): ……

1.2. Giảng viên 2:

Họ và tên: ……Nguyễn Ngọc Điệp ……

Chức danh, học hàm, học vị: ……Tiến sỹ, Giảng viên ……..

Địa điểm làm việc: Bộ môn An toàn thông tin, Khoa CNTT1,
Học viện Công nghệ Bưu chính Viễn thông

Địa chỉ liên hệ: Bộ môn An toàn thông tin, Khoa CNTT1, Cơ sở đào tạo Hà đông
Học viện Công nghệ Bưu chính Viễn thông

Điện thoại: … ..... …… Email: diepnguyenngoc@ptit.edu.vn

Các hướng nghiên cứu chính: An toàn và bảo mật thông tin, điện toán lan tỏa, học máy, khai phá dữ liệu.

Thông tin về trợ giảng (nếu có): ……

1.3. Giảng viên 3:

Họ và tên: …… Đinh Trường Duy ……

Chức danh, học hàm, học vị: ……Tiến sỹ, Giảng viên……..

Địa điểm làm việc: Bộ môn An toàn thông tin, Khoa CNTT1,
Học viện Công nghệ Bưu chính Viễn thông

Địa chỉ liên hệ: Bộ môn An toàn thông tin, Khoa CNTT1, Cơ sở đào tạo Hà đông
Học viện Công nghệ Bưu chính Viễn thông

Điện thoại: ……..……. Email: duydt@ptit.edu.vn

Các hướng nghiên cứu chính: Mạng và các giao thức, An ninh mạng, An toàn phần mềm.

Thông tin về trợ giảng (nếu có): ……

2. Thông tin chung về môn học

- Tên môn học: An toàn ứng dụng web và cơ sở dữ liệu
- Tên tiếng Anh của môn học: Web application and database security

Mã môn học: ……INT14105……..

- Số tín chỉ (TC): ……3……
- Loại môn học: ……*Bắt buộc*……

- **Các môn học tiên quyết**:
- **Môn học trước:** Mạng máy tính, Cơ sở an toàn thông tin, Cơ sở dữ liệu
- **Môn học song hành:**

- Các yêu cầu đối với môn học (nếu có):
  Phòng học lý thuyết: Có máy chiếu
  Phòngthực hành: Có máy chiếu; Hệ thống máy tính có kết nối mạng LAN và Internet
- Giờ tín chỉ đối với các hoạt động:
+ Nghe giảng lý thuyết: ……30…….. tiết
+ Bài tập, Thảo luận:……..8…..... tiết
+ Thí nghiệm, Thực hành: ……..6…. tiết
+ Tự học:……..….1…… tiết

Địa chỉ Khoa/Bộ môn phụ trách môn học:
- Địa chỉ: Bộ môn An toàn thông tin, Khoa Công nghệ thông tin 1, tầng 9, nhà A2, Cơ sở Đào tạo Hà Đông, Học viện Công nghệ BC-VT, Km 10 đường Nguyễn Trãi, Hà Nội.
- Điện thoại: 04.3854 5604

3. Mục tiêu môn học

- ***Về kiến thức:*** Trang bị cho sinh viên các kiến thức nền tảng và chuyên sâu về bảo mật cho các ứng dụng web và cơ sở dữ liệu.
- ***Kỹ năng:*** Sau khi học xong, sinh viên nắm vững các kiến thức nền tảng và chuyên sâu về bảo mật cho các ứng dụng web và cơ sở dữ liệu. Sinh viên có khả năng quản trị các máy chủ web và máy chủ cơ sở dữ liệu; phân tích và áp dụng các cơ chế/biện pháp bảo mật, đảm bảo an toàn cho máy chủ và các ứng dụng web, các cơ sở dữ liệu.
- ***Thái độ, Chuyên cần:*** đảm bảo số giờ học trên lớp và tự học.

Mục tiêu chi tiết cho từng nội dung của môn học

Mục tiêu / Nội dung	Bậc 1	Bậc 2	Bậc 3
Chương 1: Tổng quan về bảo mật ứng dụng web	- Nắm được các thành phần và kiến trúc của ứng dụng web - Nắm được các nguy cơ và lỗng hổng bảo mật ứng dụng web	- Phân tích được nguyên tắc bảo mật và các phương pháp tiếp cận bảo mật ứng dụng web	
Chương 2: Các dạng tấn công lên ứng dụng Web	- Nắm được đặc điểm các dạng tấn công phổ biến lên ứng dụng web	- Phân tích được cơ chế của các dạng tấn công phổ biến lên ứng dụng web	- Có khả năng đánh giá và lựa chọn các biện pháp phòng chống tấn công phù hợp
Chương 3: Các biện pháp bảo mật máy chủ, ứng dụng và trình duyệt web	- Nắm được các biện pháp bảo mật máy chủ và ứng dụng web - Nắm được các nguy cơ, rủi ro đối với trình duyệt web và các thành phần của nó	- Phân tích được chi tiết các biện pháp bảo mật máy chủ, ứng dụng web và khả năng áp dụng - Phân tích được chi tiết các biện pháp đảm bảo an toàn cho trình duyệt web và các thành phần của trình duyệt	- Có khả năng đánh giá và lựa chọn các biện pháp tăng cường bảo mật máy chủ và ứng dụng web - Có khả năng lựa chọn và triển khai áp dụng các biện pháp đảm bảo an toàn cho trình duyệt web
Chương 4: Bảo mật trong phát triển và triển khai ứng dụng web	- Nắm được các hướng tiếp cận trong phát triển và triển khai ứng dụng web an toàn	- Phân tích được các mô hình và phương pháp phát triển ứng dụng web an toàn	- Có khả năng đánh giá, lựa chọn áp dụng phương pháp phát triển ứng dụng web an toàn
Chương 5: Tổng quan về bảo mật cơ sở dữ liệu	- Nắm được các khái niệm về bảo mật CSDL - Nắm được yêu cầu, mô hình và các lớp bảo mật CSDL	- Phân tích được cơ chế của các dạng tấn công vào CSDL	- Có khả năng đánh giá, lựa chọn, áp dụng các biện pháp phòng chống tấn công CSDL

	- Nắm được các dạng tấn công điển hình vào CSDL và hệ quản trị CSDL		
Chương 6: Các cơ chế bảo mật cơ sở dữ liệu	- Nắm được các cơ chế, biện pháp bảo mật CSDL	- Phân tích được hệ thống các lớp biện pháp bảo mật CSDL	- Có khả năng đánh giá, lựa chọn, áp dụng các biện pháp bảo mật CSDL với từng hệ thống cụ thể
Chương 7: Sao lưu, khôi phục dự phòng, kiểm toán và giám sát hoạt động cơ sở dữ liệu	- Nắm được tầm quan trọng của vấn đề sao lưu và khôi phục dự phòng - Nắm được mục đích, vai trò của kiểm toán và giám sát CSDL	- Phân tích được các bước thực hiện sao lưu và khôi phục dự phòng CSDL - Phân tích được các bước thực hiện kiểm toán, giám sát CSDL	- Có khả năng cấu hình, thực hiện việc sao lưu, khôi phục dự phòng trên hệ thống cụ thể - Có khả năng đánh giá, lựa chọn sử dụng công cụ kiểm toán, giám sát CSDL trên hệ thống cụ thể.

4. Tóm tắt nội dung môn học

Môn học cung cấp các kiến thức nền tảng và chuyên sâu về bảo mật cho các ứng dụng web và cơ sở dữ liệu bao gồm: Các yêu cầu bảo mật các ứng dụng Web; Các nguy cơ, điểm yếu và lỗ hổng bảo mật trong các ứng dụng Web; Các phương pháp tiếp cận bảo mật các ứng dụng Web; Các dạng tấn công lên các ứng dụng Web; Các biện pháp bảo mật máy chủ, ứng dụng web và trình duyệt web; Vấn đề bảo mật trong phát triển và triển khai ứng dụng web; Các yêu cầu bảo mật CSDL, mô hình tổng quát bảo mật CSDL, các dạng tấn công thường gặp vào CSDL; Các cơ chế bảo mật CSDL;Vấn đề sao lưu, khôi phục dự phòng, kiểm toán và giám sát hoạt động của CSDL.

5. Nội dung chi tiết môn học

Phần I- An toàn ứng dụng web

Chương 1: Tổng quan về bảo mật ứng dụng web

1.1. Giới thiệu về dịch vụ web và kiến trúc các ứng dụng web
  1.1.1. Giao thức HTTP
  1.1.2. Các thành phần của ứng dụng web
  1.1.3. Kiến trúc của ứng dụng web
1.2. Các nguy cơ và lỗ hổng bảo mật trong các ứng dụng Web
  1.2.1. Giới thiệu
  1.2.2. 10 nguy cơ và lỗ hổng bảo mật hàng đầu theo OWASP
1.3. Nguyên tắc bảo mật ứng dụng Web
  1.3.1. Nguyên tắc chung
  1.3.2. Các lớp bảo mật ứng dụng web
1.4. Các phương pháp tiếp cận bảo mật các ứng dụng Web
  1.4.1. Kiểm tra dữ liệu đầu vào
  1.4.2. Giảm thiểu các giao diện có thể bị tấn công
  1.4.3. Phòng vệ có chiều sâu

Chương 2: Các dạng tấn công thường gặp lên ứng dụng web

2.1. Chèn mã HTML và Cross-Site Scripting (XSS)
  2.1.1. Khái quát về chèn mã HTML và XSS
  2.1.2. Các loại XSS
  2.1.3. Các biện pháp phòng chống
  2.1.4. Một số tấn công XSS trên thực tế
  2.1.5. Các kỹ thuật vượt qua các bộ lọc XSS
2.2. Cross-Site Request Forgery (CSRF)
  2.2.1. Giới thiệu và kịch bản
  2.2.2. Phòng chống tấn công CSRF
2.3. Tấn công chèn mã SQL

2.3.1. Khái quát
2.3.2. Vượt qua các khâu xác thực người dùng
2.3.3. Chèn, sửa đổi, hoặc xóa dữ liệu
2.3.4. Đánh cắp các thông tin trong cơ sở dữ liệu
2.3.5. Chiếm quyền điều khiển hệ thống máy chủ cơ sở dữ liệu
2.3.6. Phòng chống
2.4. Tấn công vào các cơ chế xác thực
2.4.1. Giới thiệu
2.4.2. Các dạng tấn công vào các cơ chế xác thực
2.4.3. Các biện pháp phòng chống tấn công vào các cơ chế xác thực
2.5. Tấn công khai thác các khiếm khuyết thiết kế
2.5.1. Giới thiệu
2.5.2. Một số dạng tấn công khiếm khuyết thiết kế
2.5.3. Các biện pháp phòng chống
2.6. Tấn công vào trình duyệt web và sự riêng tư của người dùng
2.6.1. Giới thiệu
2.6.2. Các dạng tấn công vào trình duyệt web và sự riêng tư của người dùng
2.6.3. Các biện pháp phòng chống
2.7. Một số ví dụ về lỗ hổng và tấn công ứng dụng web

Chương 3: Các biện pháp bảo mật máy chủ, ứng dụng và trình duyệt web

3.1. Bảo mật máy chủ web
3.1.1. Các lỗ hổng trong cấu hình máy chủ web
3.1.2. Bảo mật máy chủ web bằng cấu hình
3.1.3. Các lỗ hổng trong phần mềm máy chủ web
3.1.4. Bảo mật phần mềm máy chủ web
3.2. Bảo mật ứng dụng web
3.2.1. Bảo mật bằng xác thực và trao quyền
3.2.2. Bảo mật phiên làm việc
3.2.3. Bảo mật cơ sở dữ liệu web
3.2.4. Bảo mật hệ thống file
3.3. Bảo mật trình duyệt web
3.3.1. Các vấn đề bảo mật trình duyệt web
3.3.2. Các biện pháp bảo mật trình duyệt web

Chương 4: Bảo mật trong phát triển và triển khai ứng dụng web

4.1. Các hướng tiếp cận trong phát triển và triển khai ứng dụng web an toàn
4.1.1. Giới thiệu
4.1.2. Hướng tiếp cận toàn diện vấn đề an toàn ứng dụng
4.2. Các mô hình và phương pháp phát triển phần mềm an toàn
4.2.1. Microsoft SDL
4.2.2. OWASP CLASP
4.2.3. SAMM

Phần II- An toàn cơ sở dữ liệu

Chương 5: Tổng quan về bảo mật cơ sở dữ liệu

5.1. Các khái niệm chung
5.2. Các yêu cầu bảo mật CSDL
5.3. Mô hình tổng quát và các lớp bảo mật CSDL
5.3.1. Bảo mật cơ sở dữ liệu và các yếu tố liên quan
5.3.2. Mô hình bảo mật cơ sở dữ liệu tổng quát
5.3.3. Các lớp bảo mật cơ sở dữ liệu
5.4. Các dạng tấn công thường gặp lên CSDL

5.4.1. Các dạng tấn công thường gặp
5.4.2. 10 lỗ hổng bảo mật CSDL hàng đầu

Chương 6: Các cơ chế bảo mật cơ sở dữ liệu

6.1. Xác thực và trao quyền trong CSDL
6.1.1. Xác thực và trao quyền trong cơ sở dữ liệu
6.1.2. Bảo mật mật khẩu cơ sở dữ liệu
6.2. Bảo mật các đối tượng trong CSDL
6.3. Sử dụng mã hóa trong CSDL
6.3.1. Giới thiệu về mã hóa cơ sở dữ liệu
6.3.2. Mã hóa dữ liệu trong bảng
6.3.3. Mã hóa toàn bộ cơ sở dữ liệu
6.3.4. Mã hóa dữ liệu trên đường truyền
6.3.5. Mã hóa dữ liệu sử dụng các thiết bị lưu trữ đặc biệt
6.4. Một số biện pháp bảo mật CSDL khác
6.5. Mô hình bảo mật ở một số hệ quản trị CSDL
6.5.1 Microsoft SQL Server
6.5.2 MySQL
6.5.3 Oracle
6.6 Kiểm tra, đánh giá bảo mật hệ thống cơ sở dữ liệu

Chương 7: Sao lưu, khôi phục dự phòng, kiểm toán và giám sát hoạt động CSDL

7.1. Sao lưu và khôi phục dự phòng
7.1.1 Giới thiệu chung
7.1.2 Sao lưu cơ sở dữ liệu
7.1.3 An toàn dữ liệu sao lưu
7.1.4 Khôi phục cơ sở dữ liệu
7.2. Kiểm toán cơ sở dữ liệu
7.2.1 Khái quát về kiểm toán bảo mật
7.2.2 Các dạng kiểm toán cơ sở dữ liệu
7.3 Giám sát hoạt động của máy chủ cơ sở dữ liệu

6. Học liệu

6.1. Học liệu bắt buộc

[1] Hoàng Xuân Dậu, Bài giảng an toàn ứng dụng web và cơ sở dữ liệu, Học viện Công nghệ BCVT, 2021.

6.2. Học liệu tham khảo

[2] Bryan Sullivan, Vincent Liu, Web Application Security, A Beginner's Guide, McGraw-Hill, 2012.

[3] Alfred Basta, Melissa Zgola, *Database Security*, Cengage Learning, 2012.

[4] Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, John Wiley & Sons, 2011.

[5] Mike Shema, Hacking Web Apps: Detecting and Preventing Web Application Security Problems, Elsevier Inc., 2012.

[6] Roberta Bragg, Mark Rhodes-Ousley and Keith Strassberg, Network Security: The Complete Reference, McGraw-Hill Osborne Media, 2013.

7. Hình thức tổ chức dạy học

7.1 Lịch trình chung:

Nội dung	Hình thức tổ chức dạy môn học	Tổng

	Lên lớp			Thực hành	Tự học	cộng
	Lý thuyết	Bài tập	Thảo luận			
Nội dung 1: Tổng quan về bảo mật ứng dụng web	2					2
Nội dung 2: Chèn mã HTML và Cross-Site Scripting (XSS)	2					2
Nội dung 3: XSS và Cross-Site Request Forgery (CSRF)	2	2				4
Nội dung 4: Tấn công chèn mã SQL	2		2			4
Nội dung 5: Tấn công vào các cơ chế xác thực, Tấn công lợi dụng các khiếm khuyết thiết kế	2					2
Nội dung 6: Một số case-studies về lỗ hổng và tấn công ứng dụng web	2					2
Nội dung 7: Bảo mật máy chủ web	2					
Nội dung 8: Bảo mật phiên làm việc	2			2		4
Nội dung 9: Bảo mật trình duyệt web	2			2		4
Nội dung 10: Bảo mật trong phát triển và triển khai ứng dụng web	2	2				4
Nội dung 11: Tổng quan về bảo mật cơ sở dữ liệu	2					2
Nội dung 12: Xác thực và trao quyền trong CSDL; Bảo mật các đối tượng trong CSDL; Sử dụng mã hóa trong CSDL; Một số biện pháp bảo mật CSDL khác	2					2
Nội dung 13: Mô hình bảo mật ở một số hệ quản trị CSDL; Kiểm tra, đánh giá bảo mật hệ thống cơ sở dữ liệu	2	2				4
Nội dung 14: Sao lưu, khôi phục dự phòng, kiểm toán và giám sát hoạt động CSDL	2			2		4
Nội dung 15: Ôn tập và trả lời câu hỏi	2				1	3
Tổng cộng	**30**	**6**	**2**	**6**	**1**	**45**

7.2. Lịch trình tổ chức dạy học cụ thể

(được thiết kế cho từng nội dung ứng với 1 tuần học, cho đến hết môn học là 15 tuần).

Tuần 1, Nội dung: 1

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Tổng quan về an toàn ứng dụng dụng web	Đọc quyển 1, chương 1	

Tuần 2, Nội dung : 2

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú

Lý thuyết	2	- Chèn mã HTML và Cross-Site Scripting (XSS)	Đọc quyển 1, chương 2	

Tuần 3, Nội dung: 3

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Cross-Site Scripting (XSS) - Cross-Site Request Forgery (CSRF)	Đọc quyển 1, chương 2	
Bài tập	2	- Phân tích nguyên nhân và cơ chế tấn công XSS và CSRF	Chuẩn bị bài luận theo nhóm và slides báo cáo được giao	

Tuần 4, Nội dung: 4

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Các dạng tấn công chèn mã SQL và phòng chống	Đọc quyển 1, chương 2	
Thảo luận	2	- Phân tích nguyên nhân và cơ chế tấn công chèn mã SQL	Chuẩn bị nội dung thảo luận theo nhóm và slides báo cáo được giao	

Tuần 5, Nội dung: 5

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Tấn công vào các cơ chế xác thực - Tấn công lợi dụng các khiếm khuyết thiết kế	Đọc quyển 1, chương 2	

Tuần 6, Nội dung: 6

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Một số case-studies về lỗ hổng và tấn công ứng dụng web	Đọc quyển 1, chương 2	

Tuần 7, Nội dung: 7

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Bảo mật máy chủ web	Đọc quyển 1, chương 3	

Tuần 8, Nội dung: 8

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Bảo mật phiên làm việc	Đọc quyển 1, chương 3	
Thực hành	2	- Tìm hiểu các điểm yếu trong quản lý phiên - Thực hành các biện pháp nâng cao an toàn quản lý phiên	Ôn tập lý thuyết về bảo mật phiên làm việc ứng dụng web	

Tuần 9, Nội dung: 9

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Các biện pháp bảo mật trình duyệt web	Đọc quyển 1, chương 3	
Thực hành	2	- Thực hành một số biện pháp bảo mật máy chủ web và trình duyệt web	Ôn tập các biện pháp bảo mật máy chủ web và trình duyệt web	

Tuần 10, Nội dung: 10

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Bảo mật trong phát triển và triển khai ứng dụng web	Đọc quyển 1, chương 4	
Bài tập	2	- Tìm hiểu các dạng tấn công điển hình vào máy chủ web và ứng dụng web	Chuẩn bị bài luận theo nhóm và slides báo cáo được giao	

Tuần 11, Nội dung: 11

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Tổng quan về an toàn cơ sở dữ liệu	Đọc quyển 1, chương 5	

Tuần 12, Nội dung: 12

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Xác thực và trao quyền trong CSDL; - Bảo mật các đối tượng trong CSDL; - Sử dụng mã hóa trong CSDL; - Một số biện pháp bảo mật CSDL khác	Đọc quyển 1, chương 6	

Tuần 13, Nội dung: 13

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Mô hình bảo mật ở một số hệ quản trị CSDL; - Kiểm tra, đánh giá bảo mật hệ thống CSDL	Đọc quyển 1, chương 6	
Bài tập	2	- Tìm hiểu cơ chế bảo mật trong hệ quản trị CSDL Microsoft SQL Server	Chuẩn bị bài luận theo nhóm và slides báo cáo được giao	

Tuần 14, Nội dung: 14

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Sao lưu và khôi phục dự phòng - Kiểm toán cơ sở dữ liệu - Giám sát hoạt động cơ sở dữ liệu	Đọc quyển 1, chương 7	
Thực hành	2	- Thực hành sao lưu và khôi phục sao lưu dự phòng CSDL	Chuẩn bị nội dung bài thực hành	

Tuần 15, Nội dung: 15

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	Ôn tập và trả lời các câu hỏi	Chuẩn bị các câu hỏi/các nội dung chưa rõ	
Tự học/ Tự nghiên cứu	1			

8. Chính sách đối với môn học và các yêu cầu khác của giảng viên *(Phần này căn cứ vào đặc thù môn học, phương pháp tổ chức giảng dạy, giảng viên chủ động đề xuất, Riêng phần kiểm tra cuối kỳ tỷ lệ đánh giá thấp nhất là 50%)*

- Các bài tập/tiểu luận phải làm đúng hạn. Nếu không đúng hạn sẽ bị điểm 0.
- Thiếu một điểm thành phần (bài tập, bài kiểm tra giữa kỳ), hoặc nghỉ quá 20% tổng số giờ của môn học, không được thi hết môn.
- Tham gia đầy đủ và hoàn thành các bài thực hành theo yêu cầu.

9. Phương pháp, hình thức kiểm tra – đánh giá kết quả học tập môn học

9.1. Kiểm tra đánh giá định kỳ

Hình thức kiểm tra *(Tham khảo ví dụ dưới đây)*	Tỷ lệ đánh giá	Đặc điểm đánh giá
- Tham gia học tập trên lớp (đi học đầy đủ, tích cực thảo luận)	10 %	Cá nhân
- Các bài tập và thảo luận trên lớp	20%	Nhóm
- Hoạt động theo nhóm		
- Kiểm tra giữa kỳ	10%	Cá nhân
- Kiểm tra cuối kỳ	60%	Cá nhân

9.2. Nội dung và Tiêu chí đánh giá các loại bài tập

Căn cứ vào Phương án lập kế hoạch Giảng dạy trong chương trình đào tạo đã ban hành, sau các nội dung giảng dạy lý thuyết là phần Giao bài tập về nhà cho sinh viên thực hiện, Tại giờ chữa bài tập, thảo luận, Giảng viên thực hiện chữa mẫu các bài tập trên, hoặc kiểm tra đánh giá quá trình tự học ở nhà của sinh viên. Việc kiểm tra đánh giá quá trình học tập được thực hiện tại thời gian chữa bài tập/ thảo luận.

Các loại bài tập/thảo luận	Yêu cầu và Tiêu chí đánh giá
- Bài tập	- Yêu cầu sinh viên nắm vững và trình bày được kiến thức căn bản của môn học - Tìm tài liệu, tổng hợp kiến thức và viết báo cáo theo yêu cầu của bài tập được giao cho nhóm - Phân chia công việc và cộng tác theo nhóm - Chuẩn bị slides và trình bày trước lớp
- Thảo luận	- Tìm hiểu các vấn đề theo yêu cầu của nội dung thảo luận được giao và trả lời câu hỏi trực tiếp
- Kiểm tra giữa kỳ, cuối kỳ	- Nắm vững kiến thức môn học - Trả lời đúng các câu hỏi và bài tập

Duyệt	**Chủ nhiệm bộ môn**	**Giảng viên** *(Chủ trì biên soạn đề cương)*
TS Nguyễn Duy Phương	**TS. Nguyễn Ngọc Điệp**	**TS. Hoàng Xuân Dậu**