ĐẠI HỌC ĐÀ NẴNG
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG VIỆT - HÀN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

CHƯƠNG TRÌNH GIÁO DỤC ĐẠI HỌC

Trình độ đào tạo: Đại học Ngành: Kỹ sư Công nghệ thông tin Mã số:
Chuyên ngành: Mạng và An toàn thông tin

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

1. Thông tin chung về học phần

1.1.	**Mã học phần:**	**1.2. Tên học phần: An toàn ứng dụng web và cơ sở dữ liệu**
1.3.	**Ký hiệu học phần:**	**1.4. Tên tiếng Anh: Database and Web Application Security**
1.5.	**Số tín chỉ:**	2 TC
1.6.	**Phân bố thời gian:**	
-	Lý thuyết:	1.5 TC (21 tiết)
-	Bài tập/Thảo luận:	
-	Thực hành/Thí nghiệm:	0.5 TC (9 tiết)
-	Tự học:	90 tiết
1.7.	**Các giảng viên phụ trách học phần:**	
-	Giảng viên phụ trách chính:	ThS. Trần Thanh Liêm
-	Danh sách giảng viên cùng giảng dạy:	TS. Hoàng Hữu Đức; ThS. Lê Kim Trọng; ThS. Đỗ Công Đức; ThS. Ninh Khánh Chi; TS. Đặng Quang Hiển; ThS. Lê Tự Thanh.
-	Bộ môn phụ trách giảng dạy:	
1.8.	**Điều kiện tham gia học phần:**	
-	Học phần tiên quyết:	
-	Học phần học trước:	
-	Học phần song hành:	
1.9	**Loại học phần:**	Tự chọn bắt buộc
1.10	**Thuộc khối kiến thức**	Kiến thức Chuyên ngành

2. Mục tiêu học phần

II.1. Mục tiêu chung

Hiện nay, các ứng dụng web từ các phần mềm quản lý nội bộ đến các hệ thống quản lý tài chính, từ các ứng dụng thương mại điện tử đến các hệ thống giao dịch ngân hàng, bao gồm quy mô sử dụng trong hệ thống mạng nội bộ đến cung cấp rộng rãi cho người dùng internet đang đối mặt với các vụ tấn công, xâm hại vào các máy chủ và website. Xuất phát từ thực tế đó, khóa học "Bảo mật ứng dụng Web" được thiết kế đặc biệt, cung cấp học viên kiến thức, kinh nghiệm về cấu hình, cài đặt, bảo trì và nâng cao tính năng bảo mật cho máy chủ và các ứng dụng web nhằm đảm bảo an toàn trước nguy cơ tấn công thông qua website của cơ quan, doanh nghiệp

II.2. Mục tiêu cụ thể

II.2.1. Về kiến thức

- CO1: Trang bị cho sinh viên kiến thức chuyên sâu về An toàn ứng dụng web và cơ sở dữ liệu như: các kỹ thuật mật mã, an toàn cơ sở dữ liệu, an toàn các ứng dụng Web và Internet, lập trình an toàn, thiết kế các phần mềm và công cụ đảm bảo an toàn, quản lý và đánh giá điểm yếu, các kỹ thuật kiểm tra đánh giá an toàn, các vấn đề về chính sách, pháp luật …

II.2.2. Về kỹ năng

- CO2: Áp dụng các kiến thức, kỹ năng; sử dụng các công cụ khoa học kỹ thuật để nhận biết, phân tích, giải quyết vấn đề liên quan đến an toàn ứng dụng web và cơ sở dữ liệu;
- CO3: Thiết kế và triển khai các ứng dụng đảm bảo an toàn ứng dụng web và cơ sở dữ liệu đáp ứng các yêu cầu kỹ thuật đặt ra trong điều kiện thực tế;
- CO4: Tìm kiếm, tiếp cận, ứng dụng hiệu quả các kỹ thuật, kỹ năng và công cụ hiện đại để giải quyết những vấn đề thực tế của an toàn ứng dụng web và cơ sở dữ liệu.

II.2.3. Về thái độ

- CO5: Giúp sinh viên phát triển được thái độ tốt, có ý thức chủ động, trách nhiệm và tôn trọng lẫn nhau trong học tập.

II.3. Mô tả tóm tắt học phần: nội dung học phần gồm 4 chương.

- Chương 1. TỔNG QUAN VỀ BẢO MẬT
- Chương 2. WEB SERVER VÀ GIAO THỨC HTTPS
- Chương 3. TẤN CÔNG VÀ BẢO MẬT ỨNG DỤNG WEB
- Chương 4. TẤN CÔNG VÀ BẢO MẬT CƠ SỞ DỮ LIỆU

3. Chuẩn đầu ra của học phần

Học xong học phần, sinh viên có khả năng:

Số TT	Ký hiệu CĐR học phần (CLO)	Chuẩn đầu ra học phần (CLOs)	Nhận thức	Kỹ năng	Mức tự chủ và chịu trách nhiệm
1	CLO1	Nắm được về "Web hacking", các kiểu xâm nhập như SQL Injection, Session Hijack, DoS, Social Engineering v.v…	CO1		
2	CLO2	Áp dụng được https và cấu hình sử dụng trên Web Server	CO1		
3	CLO3	Giải quyết các lỗi bảo mật trên ứng dụng web và cách phòng chống thông	CO1 CO2		

		qua các phần mềm chuyên dụng để quét lỗi hệ thống.			
4	CLO4	Giải quyết các dạng tấn công dữ liệu và cách hạn chế lỗi bảo mật trên các máy chủ dữ liệu.	CO1 CO2		
5	CLO5	Xây dựng các giải pháp phòng chống đảm bảo an toàn cho hệ thống Web		CO3 CO4	
6	CL06	Thể hiện thái độ và trách nhiệm làm việc theo nhóm.			CO5

4. Mối liên hệ giữa chuẩn đầu ra học phần (CLOs) và chuẩn đầu ra chương trình đào tạo (PLOs):

Mức độ đóng góp, hỗ trợ của CLO đối với PLO được xác định cụ thể như sau:

Điền một trong các mức I, R, M hoặc chừa trống (nếu không có sự liên hệ) và điền A vào ô tương ứng

Chuẩn đầu ra học phần (CLOs)	**Chuẩn đầu ra CTĐT (PLOs)**							
	PLO1	**PLO2**	**PLO3**	**PLO4**	**PLO5**	**PLO6**	**PLO7**	**PLO 8**
CLO 1			**I**	**R**				
CLO 2			**I**	**M**				
CLO 3		**I**	**I**		**I**			
CLO 4		**I**	**I**		**I**			
CLO 5		**R**	**I**			**I**	**R**	**I**
CLO 6	**I**	**I**						

Chú thích:

- *I (Introduced) – CLO có hỗ trợ đạt được PLO và ở mức giới thiệu/bắt đầu*
- *R (Reinforced) – CLO có hỗ trợ đạt được PLO và ở mức nâng cao hơn mức bắt đầu, có nhiều cơ hội được thực hành, thí nghiệm, thực tế,…*
- *M (Mastery) – CLO hỗ trợ mạnh mẽ người học trong việc thuần thục/thành thạo hay đạt được PLO/PI. Nếu người học hoàn thành tốt CLO này thì xem như người học đã ở mức thuần thục/thành thạo một nội hàm quan trọng (PI) của PLO hoặc thâm chí thuần thục/thành thạo toàn bộ PLO đó.*

- *A (Assessed) – CLO quan trọng (hỗ trợ tối đa việc đạt được PLO) cần được thu thập dữ liệu để đo lường đánh giá mức độ người học đạt được PLO.*

5. Đo lường đánh giá mức độ người học đạt chuẩn đầu ra của học phần (gọi tắt là đánh giá CLO)

CLO	Nội dung CLO	Sự cần thiết để đánh giá CLO	Có hỗ trợ đánh giá PLO		Dữ liệu để đánh giá CLO được lấy từ	Mục tiêu đối với CLO
			PI	Nội dung PI		
CLO5	Sử dụng được các công cụ để xây dựng các giải pháp phòng chống cho hệ thống.				thi cuối kỳ	

6. Đánh giá học phần

6.1. Phương pháp, hình thức kiểm tra – đánh giá của học phần

Kết quả học tập của sinh viên được đánh giá bằng các thành phần: đánh giá quá trình, đánh giá giữa kỳ, đánh giá cuối kỳ, các hoạt động đánh giá khác...

Thành phần đánh giá	Trọng số (%)	Hình thức đánh giá	Trọng số con (%)	Rubric (đánh dấu X nếu có)	Chuẩn đầu ra học phần có liên quan	Hướng dẫn phương pháp đánh giá
(1)	(2)	(3)	(4)	(5)	(6)	(7)
A1. Đánh giá chuyên cần	10%	Có ý thức tham gia học tập đầy đủ, hoàn thành đúng hạn các yêu cầu của giảng viên và tích cực phát biểu ý kiến			CLO 1 CLO 2 CLO 3 CLO 4 CLO 5	
A2. Đánh giá định kỳ	40%	Kiểm tra giữa kỳ			CLO 3 CLO 4	*SV làm bài thực hành hành theo yêu cầu và hướng dẫn của GV. GV sẽ chấm điểm căn cứ vào kiến thức, kỹ năng*

Thành phần đánh giá	Trọng số (%)	Hình thức đánh giá	Trọng số con (%)	Rubric (đánh dấu X nếu có)	Chuẩn đầu ra học phần có liên quan	Hướng dẫn phương pháp đánh giá
A3. Đánh giá cuối kỳ	50%	Bài thi cuối kỳ: Thi thực hành cuối kỳ.			CLO 3 CLO 4 CLO 5 CLO 6	*Bài thi cuối kỳ GV sẽ chấm kết quả thực hiện bài thi thực hành của sinh viên.*

6.2. Chính sách đối với học phần

SV tham dự >=80% số buổi của HP. Nếu nghỉ >20% số buổi sẽ không được tham gia thi thực hành cuối học kỳ.

7. Kế hoạch và nội dung giảng dạy học phần

Tuần/ Buổi (3 tiết/buổi)	Các nội dung cơ bản của bài học (chương)	Số tiết (LT/TH/TT)	CĐR học phần có liên quan	PP giảng dạy đạt CĐR	Hoạt động học của SV	Hình thức đánh giá
(1)	(2)	(3)	(4)	(5)	(6)	(7)
1	**Chương 1. TỔNG QUAN VỀ BẢO MẬT** 1.1. Giới thiệu về bảo mật 1.2. Những tài nguyên cần bảo vệ 1.3. Những lỗ hỏng bảo mật 1.4. Các kiểu tấn công của hacker 1.5. Các biện pháp phát hiện hệ thống bị tấn công 1.6. Các quy tắc bảo mật 1.7. Xây dựng chính sách bảo mật	3 LT	CLO 1	Phương pháp: Giảng theo slide, hướng dẫn ví dụ thực hành trực tiếp trên lớp.	Nghe giảng, hiểu được tổng quan về bảo mật	A1.1, A1.2
2	**Chương 2. WEB SERVER VÀ GIAO THỨC HTTPS** 2.1. Quét máy chủ web và các lỗi bảo	3 LT	CLO 2	Phương pháp: Giảng theo slide, hướng dẫn ví dụ thực	Nghe giảng hiểu, nắm bắt được chứng thực và SSL	A1.1, A1.2

Tuần/ Buổi (3 tiết/buổi)	Các nội dung cơ bản của bài học (chương)	Số tiết (LT/TH/TT)	CĐR học phần có liên quan	PP giảng dạy đạt CĐR	Hoạt động học của SV	Hình thức đánh giá
	mật phổ biến trên webserver 2.2. Cách phòng chống 2.3. Chứng thực và các loại chứng thực. 2.4. SSL (Secure Socket Layer) và nhu cầu của chứng thực dịch vụ dựa trên SSL 2.5. Cấp chứng nhận cho máy chủ ứng dụng: HTTPS, FTPS, …			hành trực tiếp trên lớp.		
3	**Chương 2. WEB SERVER VÀ GIAO THỨC HTTPS** 2.6. Kiểm tra và phân tích hiện trạng của web server 2.7. Cài đặt Enterprise Certificate Authority,… 2.8. Cấp chứng chỉ cho máy chủ IIS. 2.9. Kiểm tra vận hành ứng dụng trên giao thức HTTPS.	3 LT	CLO 2	Phương pháp: Giảng theo slide, hướng dẫn ví dụ thực hành trực tiếp trên lớp.	Nghe giảng hiểu, nắm bắt được một số cách cài đặt chứng chỉ, và vận hành ứng dụng giao thức https	A1.1, A1.2
4	**Bài thực hành 01.** Chuẩn bị và làm quen với các công cụ học tập và công cụ tạo máy ảo	3 TH	CLO 1, 2	Phương pháp: Hướng dẫn ví dụ thực hành trực tiếp trên lớp.	Cài đặt và thực hành được các công cụ tạo máy ảo	A1.1, A1.2
5	**Chương 3. TẤN CÔNG VÀ BẢO MẬT ỨNG DỤNG WEB** 3.1. Các vấn đề an toàn ứng dụng web	3 LT	CLO 1, 2, 3, 5, 6	Phương pháp: Giảng theo slide, hướng dẫn ví dụ thực	Nghe giảng hiểu, nắm bắt được một số cách bẻ khóa, tấn công chèn	A1.1, A1.2, A1.3

Tuần/ Buổi (3 tiết/buổi)	Các nội dung cơ bản của bài học (chương)	Số tiết (LT/TH/TT)	CĐR học phần có liên quan	PP giảng dạy đạt CĐR	Hoạt động học của SV	Hình thức đánh giá
	hiện tại và xu hướng. 3.2. Các tiêu chí đánh giá hệ thống ứng dụng web an toàn 3.3. Kiểm tra lỗi bảo mật cho ứng dụng web 3.4. Các phương pháp xác thực web cơ bản 3.5. Kỹ thuật bẻ khóa mật khẩu web 3.6. Kỹ thuật tấn công bằng cách chèn những đoạn mã script vào các website (XSS) 3.7. Biện pháp phòng chống			hành trực tiếp trên lớp.	đoạn mã script	
6	**Chương 3. TẤN CÔNG VÀ BẢO MẬT ỨNG DỤNG WEB** 3.8. Dò lỗi hệ thống 3.9. Xây dựng web server giả mạo 3.9. Tấn công giả mạo trang Web (Web Phishing Attack) 3.10. Phòng chống và khắc phục: 3.11. Các module nguồn mở dễ bị tấn công và cách khắc phục, phòng chống: CKEditor,…	3 LT	CLO 1, 2, 3, 5, 6	Phương pháp: Giảng theo slide, hướng dẫn ví dụ thực hành trực tiếp trên lớp.	Nghe giảng hiểu, nắm bắt được cách dò lỗi hệ thống và cách khắc phục, phòng chống	A1.1, A1.2, A1.3
7	**Bài thực hành 02.** Cài đặt hệ điều hành, cài đặt web server, các dịch vụ như SSL ... sử dụng các công cụ để bẻ	3 TH	CLO 1, 2, 3, 5, 6	Phương pháp: Hướng dẫn ví dụ thực hành	Cài đặt và thực hành được các dịch vụ như SSL, công cụ để bẻ	A1.1, A1.2, A1.3

Tuần/ Buổi (3 tiết/buổi)	Các nội dung cơ bản của bài học (chương)	Số tiết (LT/TH/TT)	CĐR học phần có liên quan	PP giảng dạy đạt CĐR	Hoạt động học của SV	Hình thức đánh giá
	khóa mật khẩu và cách phòng chống.			trực tiếp trên lớp.	khóa mật khẩu. Xây dựng phương án phòng chống.	
8	**Chương 4. TẤN CÔNG VÀ BẢO MẬT CƠ SỞ DỮ LIỆU** 4.1. Cơ sở dữ liệu phổ biến 4.2. Các dạng tấn công cơ sở dữ liệu phổ biến 4.3. Kỹ thuật khai thác lỗi SQL Injection 4.4. Công cụ tấn công SQL Injection 4.5. Biện pháp phòng chống	3 LT	CLO 1, 2, 4, 5, 6	Phương pháp: Giảng theo slide, hướng dẫn ví dụ thực hành trực tiếp trên lớp.	Nghe giảng nắm bắt được các dạng tấn công cơ sở dữ liệu phổ biến	A1.1, A1.2, A1.3
9	**Chương 4. TẤN CÔNG VÀ BẢO MẬT CƠ SỞ DỮ LIỆU** 4.6. Tìm kiếm những website bị lỗi SQL Injection. 4.7. Khai thác các công cụ dò lỗi SQL Injection: Vega, Zed attack proxy, Wapiti, AppScan, SQLMap. 4.8. Khai thác lỗ hổng SQL Injection 4.9. Phòng chống SQL Injection	3 LT	CLO 1, 2, 4, 5, 6	Phương pháp: Giảng theo slide, hướng dẫn ví dụ thực hành trực tiếp trên lớp.	Nghe giảng nắm bắt được SQL Injection và cách phòng chống	A1.1, A1.2, A1.3
10	**Bài thực hành 03.** Xây dựng một cơ sở dữ liệu cơ bản và sử dụng kỹ thuật khai thác lỗi SQL Injection. Sau đó	3 TH	CLO 1, 2, 4, 5, 6	Phương pháp: Hướng dẫn ví dụ thực hành	Cài đặt và thực hành được SQL Injection và đưa ra các biện pháp	A1.1, A1.2, A1.3

Tuần/ Buổi (3 tiết/buổi)	Các nội dung cơ bản của bài học (chương)	Số tiết (LT/TH/TT)	CĐR học phần có liên quan	PP giảng dạy đạt CĐR	Hoạt động học của SV	Hình thức đánh giá
	đưa ra biện pháp phòng chống.			trực tiếp trên lớp.	phòng chống	
Theo lịch thi	Thi cuối kỳ					

Ghi chú:

- (3) Số tiết (LT/TH/TT): Xác định số tiết lý thuyết, thực hành, thực tập của từng chương

- (5) PP giảng dạy đạt CĐR: Nêu tên các PP giảng dạy sử dụng trong từng chương để đạt CĐR

- (6) Hoạt động học của SV: Xác định các nội dung SV cần chuẩn bị tại nhà (đọc tài liệu nào, từ trang thứ mấy, làm việc nhóm để giải quyết BT, làm dự án ……..); Hoạt động tại lớp (thảo luận nhóm, làm BT thường xuyên số….).

8. Báo cáo đánh giá chuẩn đầu ra học phần sau khi có kết quả thi kết thúc học phần *(chi tiết phụ lục đính kèm)*

9. Học liệu

9.1. Sách, giáo trình, tài liệu tham khảo

TT	Tên tác giả	Năm XB	Tên sách, giáo trình, tên bài báo, văn bản	NXB, tên tạp chí/ nơi ban hành VB
	Sách, bài giảng, giáo trình chính			
1	Hoàng Xuân Dậu	2017	An toàn ứng dụng web và cơ sở dữ liệu	Học viện Công nghệ Bưu chính Viễn thông
	Sách, giáo trình tham khảo			
2	Bryan Sullivan, Vincent Liu	2012	Web Application Security, A Beginner's Guide	McGraw-Hill, New York City
3	Andrew Homan	2020	Web Application Security, Exploitation and Countermeasures for Modern Web Applications	O'Reilly Media
4	Dafydd Stuttard, Marcus Pinto	2011	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws	John Wiley & Sons
5	Mike Shema	2012	Hacking Web Apps: Detecting and Preventing Web Application Security Problems	Elsevier Inc.
6	Nhóm GV VKU	2023	Bài giảng An toàn ứng dụng web và cơ sở dữ liệu	

9.2. Danh mục địa chỉ website để tham khảo khi học học phần

TT	Nội dung tham khảo	Link trang web	Ngày cập nhật
1			
2			

10. Cơ sở vật chất phục vụ giảng dạy

TT	Tên giảng đường, PTN, xưởng, cơ sở TH	Danh mục trang thiết bị, phần mềm chính phục vụ TN,TH		Phục vụ cho nội dung Bài học/Chương
		Tên thiết bị, dụng cụ, phần mềm,…	Số lượng	

1				
2				

11. Rubric đánh giá làm việc nhóm qua bài tập lớn (dự án)

Tiêu chí đánh giá	MỨC D (4.0-5.4)	MỨC C (5.5-6.9)	MỨC B (7.0-8.4)	MỨC A (8.5-10)
Nội dung (80%)	Sản phẩm không vận hành được hoặc còn nhiều lỗi.	Đạt mục tiêu project, còn 1 vài lỗi nhỏ chấp nhận được. Trả lời 50% câu hỏi của giảng viên.	Đạt mục tiêu project, còn 1 vài lỗi nhỏ chấp nhận được. Trả lời hết các câu hỏi của giảng viên.	Đạt mục tiêu project, hoàn toàn tốt, đầy đủ. Trả lời hết các câu hỏi của giảng viên.
Làm việc nhóm (20%)	Ít tham gia	Có hợp tác, có tham gia	Chủ động tham gia	Tham gia tích cực

Đà Nẵng, ngày tháng năm 2023

Trưởng khoa	Trưởng bộ môn	Giảng viên biên soạn
TS. Nguyễn Vũ Anh Quang		**ThS. Trần Thanh Liêm**