TRƯỜNG ĐẠI HỌC VĂN HIẾN
KHOA: CÔNG NGHỆ THÔNG TIN

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

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

1. Thông tin về học phần

- Tên học phần: Bảo mật Web và Ứng dụng (Web Application Security)
- Mã học phần: INT491
- Số tín chỉ: 2 (2/0/4)
- Bậc đào tạo: Đại học
- Loại học phần: Bắt buộc
- Học phần tiên quyết/ Học phần trước: An toàn mạng máy tính
- Đơn vị phụ trách: Khoa Công Nghệ Thông Tin
- Số giờ tín chỉ: 30, trong đó:
- Lý thuyết: 30 tiết
- Thực hành: 0 tiết
- Thực tập: 0 tiết
- Đồ án/ Khóa luận 0 tiết

2. Thông tin về giảng viên

Giảng viên 1:

- Họ và tên: Nguyễn Quang Tấn
- Chức danh, học vị: Tiến sĩ
- Thời gian làm việc: Giờ hành chính (8:00 -16:00)
- Địa điểm làm việc: Khoa Công Nghệ Thông Tin; Trường Đại học: Đại Văn Hiến
- Điện thoại: 0903766808
- Email: tannq@vhu.edu.vn

Giảng viên 2:

- Họ và tên: .....
- Chức danh, học vị: .....
- Thời gian làm việc: Giờ hành chính (8:00 -16:00)
- Địa điểm làm việc: Khoa ….. - Trường Đại học …..
- Điện thoại: .....
- Email: .....

3. Tóm tắt nội dung học phần

Học phần gồm 6 chương, trình bày nhu cầu triển khai ứng dụng web an toàn trong môi trường mạng internet hiện nay; các kỹ thuật bảo vệ cốt lõi mà ứng dụng web hỗ trợ; các kỹ thuật tấn công ứng dụng web như: lập bản đồ ứng dụng web, tấn công bỏ qua sự điều khiển, tấn công chứng thực, tấn công phiên làm việc, tấn công cơ sở dữ liệu, tấn công người sử dụng, tấn công giả mạo dữ liệu, …; các kỹ thuật quét lỗi cơ bản; các kỹ thuật mã hóa dữ liệu; các kỹ thuật quét lỗi tự động và quét lỗi nhiều mặt. Ngoài ra, học phần còn rèn luyện kỹ năng giải quyết các vấn đề thường gặp trong An toàn mạng và tạo ham mê học tập cũng như xây dựng các ứng dụng thực tế.

4. Mục tiêu của học phần

Học phần có những mục tiêu:

- Cung cấp cho người học những kiến thức chung về tổng quát về mạng máy tính, Tổng quan về cấu trúc của mạng máy tính, các thành phần cơ bản của một mạng, giao thức mạng phổ biến, và các thiết bị mạng cơ bản.

- Cung cấp kiến thức cho sinh viên về các lỗ hổng bảo mật trong ứng dụng web, các kỹ thuật phát hiện và giải pháp khắc phục.

- Trang bị kiến thức về kỹ năng Áp dụng kiến thức vào Thực hành: Thực hành khám phá các kỹ thuật và giải pháp khắc phục thông qua các bài tập và dự án thực tế. Do vậy, sinh viên có thể làm việc được ngay sau khi ra trường vì nhu cầu xã hội về độ ngũ phát triển hoặc kiểm tra lỗi bảo mật web ra rất cao trong xã hội Internet hiện nay.

- Phát triển kỹ năng phân tích, lập luận, và thuyết trình hiệu quả.

5. Chuẩn đầu ra của học phần:

Mã CĐR	**Nội dung chuẩn đầu ra** (Bắt đầu bằng động từ theo thang Bloom)
Kiến thức	
CLO1	Giải quyết vấn đề dựa trên các kỹ năng định lượng và kiến thức về logic cơ bản, giải tích, thống kê
CLO2	Phân tích các vấn đề trong thực tế dựa trên kiến thức cơ bản về khoa học tự nhiên, phương pháp tính toán, kiến thức vật lý.
CLO3	Trình bày được các kiến thức trải nghiệm ngành nghề, các kiến thức cơ bản và phương pháp học tập của chuyên ngành
CLO4	Sử dụng thành thạo các phần mềm phát hiện lỗ hổng bảo mật, kỹ thuật khảo sát, đánh giá và tính toán cho thiết kế an toàn hệ thống web. Giải quyết các vấn đề cơ bản trong lĩnh vực công nghệ thông tin

CLO5	Sử dụng thành thạo các phần mềm giám sát mạng, lập trình Web, hệ điều hành mã nguồn mở. Phát hiện và sửa đổi, giải quyết được các lỗi lập trình hoặc hệ điều hành.
Kỹ năng	
CLO6	Tham gia làm việc nhóm và có những đóng góp mang lại hiệu quả.
CLO7	Sử dụng các ứng dụng CNTT thành thạo.
CLO8	Xác định, so sánh các công nghệ mới, các xu thế phát triển trong quá trình học tập.
CLO9	Thực hiện thành thạo các kỹ năng nghiệp vụ chuyên môn, chuyên ngành.
Mức tự chủ và trách nhiệm	
CLO10	Giữ gìn đạo đức nghề nghiệp.
CLO11	Có ý thức đóng góp tạo ra những sản phẩm có giá trị, góp phần thúc đẩy sự phát triển khoa học và kỹ thuật đất nước.
CLO12	Có thói quen học tập suốt đời.

Ma trận liên kết giữa Chuẩn đầu ra chương trình đào tạo và Chuẩn đầu ra học phần

Chuẩn đầu ra	**PLO1**	**PLO2**	**PLO3**	**PLO4**	**PLO5**	**PLO6**	**PLO7**	**PLO8**	**PLO9**	**PLO10**
CLO1	X									
CLO2	X									
CLO3	X									
CLO4		X								
CLO5		X								
CLO6					X					
CLO7							X			
CLO8							X			
CLO9								X		
CLO10									X	
CLO11									X	
CLO12										X

***Ghi chú: PLOs** (Programme Learning Outcomes): Chuẩn đầu ra cấp CTĐT*

***CLOs** (Course Learning Outcomes): Chuẩn đầu ra học phần*

6. Nội dung chi tiết của học phần

6.1. Lý thuyết

Chương	Nội dung	Đáp ứng CLOs
Chương 1	**TỔNG QUAN VỀ BẢO MẬT WEB**	**CLO2, CLO4**
1.1.	Giới thiệu về Internet và an toàn Web	
1.2.	Các chức năng thông dụng của ứng dụng web	
1.3.	Ưu điểm của ứng dụng web	
1.4.	Tính an toàn của ứng dụng web	
1.5.	Các nguy cơ và giải pháp bảo vệ	
Chương 2	**CÁC CƠ CHẾ BẢO VỆ CỐT LÕI CỦA WEB**	**CLO2, CLO5**
2.1.	Kiểm soát sự truy cập của người dùng	
2.2.	Kiểm soát dữ liệu nhập	
2.3.	Kiểm soát tấn công	
2.4.	Quản lý ứng dụng	
Chương 3	**BẢN ĐỒ ỨNG DỤNG WEB VÀ CÁC KỸ THUẬT BỎ QUA SỰ ĐIỀU KHIỂN PHÍA CLIENT**	**CLO2, CLO5**
3.1.	Thu thập nội dung và chức năng của ứng dụng web.	
3.2.	Phân tích ứng dụng web.	
3.3.	Truyền dữ liệu thông qua client.	
3.4.	Bắt dữ liệu người dùng.	
3.5.	Kiểm soát an toàn dữ liệu phía máy khách	
Chương 4	**CÁC KỸ THUẬT TẤN CÔNG CHỨNG THỰC VÀ TẤN CÔNG PHIÊN LÀM VIỆC**	**CLO2, CLO5**
4.1.	Các công nghệ chứng thực	
4.2.	Thiết kế cơ chế tấn công chứng thực	
4.3.	Giải pháp an toàn chứng thực.	
4.4.	Nhu cầu duy trì trạng thái.	
4.5.	Điểm yếu của việc phát sinh và kiểm soát mã phiên giao tiếp	
4.6.	Giải pháp quản lý an toàn phiên giao tiếp	
Chương 5	**CÁC KỸ THUẬT TẤN CÔNG KIỂM SOÁT TRUY CẬP, TẤN CÔNG CSDL VÀ TẤN CÔNG LOGIC ỨNG DỤNG**	**CLO2, CLO5**
5.1.	Các kỹ thuật tấn công kiểm soát truy cập và giải pháp	

Chương	Nội dung	Đáp ứng CLOs
5.2.	Tấn công chèn vào ngữ cảnh giao tiếp	
5.3.	Tấn công chèn mã độc SQL	
5.4.	Tấn công chèn mã độc không SQL	
5.5.	Tấn công XPath	
5.6.	Tấn công LDAP	
Chương 6	**CÁC KỸ THUẬT TẤN CÔNG NGƯỜI SỬ DỤNG: XSS VÀ CÁC KỸ THUẬT KHÁC**	**CLO2, CLO5**
6.1.	Tổng quan XSS (Cross-Site-Scripting)	
6.2.	Các kỹ thuật tấn công XSS	
6.3.	Giải pháp ngăn chặn tấn công XSS	
6.4.	Tấn công trình duyệt	
6.5.	Tấn công ActiveX Controls	
6.6.	Tấn công AJAX	

6.2. Thực hành

	Nội dung	Đáp ứng CLOs
6.2.1.	**Bài tập cá nhân**	**CLO2, CLO5**
	Người học thực hiện ít nhất 01 bài cá nhân theo yêu cầu giảng viên	
6.2.2.	**Bài tập nhóm**	**CLO2, CLO5**
	- Người học thực hiện 01 bài tập nhóm - Các nhóm báo cáo kết quả làm việc trước lớp.	

7. Phân bổ thời gian theo tiết và điều kiện thực hiện:

STT	Tên chương	Số tiết tín chỉ					Ghi chú
		Lý thuyết	Bài tập	Thực hành	Tự học	Tổng	
1	**Tổng quan về bảo mật web**	04	0	0	10	14	
2	**Các cơ chế bảo vệ cốt lõi của web**	05	0	0	10	15	

STT	Tên chương	Số tiết tín chỉ					Ghi chú
		Lý thuyết	Bài tập	Thực hành	Tự học	Tổng	
3	**Bản đồ ứng dụng web và các kỹ thuật bỏ qua sự điều khiển phía client**	04	0	0	10	13	
4	**Các kỹ thuật tấn công chứng thực và tấn công phiên làm việc**	06	0	0	10	17	
5	**Các kỹ thuật tấn công kiểm soát truy cập, tấn công CSDL và tấn công logic ứng dụng**	04	0	0	10	14	
6	**Các kỹ thuật tấn công người sử dụng: xss và các kỹ thuật khác**	07	0	0	10	17	
Tổng		**30**	**0**	**0**	**60**	**90**	

CÁC CHỦ ĐỀ THẢO LUẬN VÀ TIỂU LUẬN

1. .....
2. .....
3. .....

8. Phương pháp giảng dạy:

Giảng viên giảng dạy với sự kết hợp của một số phương pháp sau:

Gợi ý:

- Thuyết trình
- Phát vấn
- Hỏi lại hoặc vấn đáp
- Đọc và tóm lược nội dung tài liệu
- Động não nhanh (bài tập tư duy cá nhân)
- Giao bài đọc về nhà
- Hướng dẫn tự học
- Thảo luận nhóm

Ma trận liên kết giữa Chuẩn đầu ra với phương pháp giảng dạy

Phương pháp giảng dạy	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7	CLO8	CLO9	CLO10	CLO11	CLO12
Thuyết trình	X	X	X	X	X		X	X		X	X	
Phát vấn	X			X	X	X	X					X
Hỏi lại hoặc vấn đáp	X	X	X	X	X	X	X		X		X	X
Đọc và tóm lược nội dung tài liệu	X	X	X	X	X			X	X	X	X	

9. Phương pháp học tập

Sinh viên học tập với sự kết hợp của một số phương pháp sau:

Gợi ý:

- Thuyết trình
- Làm việc nhóm
- Tự học, tự nghiên cứu

Ma trận liên kết giữa Chuẩn đầu ra với phương pháp học tập

Phương pháp học tập	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7	CLO8	CLO9	CLO10	CLO11	CLO12
Thuyết trình	X		X		X			X		X	X	X
Làm việc nhóm	X		X	X		X						
Tự học, tự nghiên cứu	X	X	X	X	X	X	X	X	X	X	X	X

10. Nhiệm vụ của sinh viên

Gợi ý:

- Chủ động tổ chức thực hiện giờ tự học.
- Tham gia đầy đủ các giờ lên lớp và giờ thuyết trình (sinh viên chỉ được vắng mặt tối đa 20% thời gian lên lớp của học phần).

- Đọc tài liệu tham khảo bắt buộc và bổ trợ do giảng viên giới thiệu.
- Hoàn thành đầy đủ các bài tập cá nhân, bài tập nhóm.
- Tham gia kỳ thi kết thúc học phần.

11. Thang điểm đánh giá: Điểm đánh giá quá trình và điểm thi kết thúc học phần được chấm theo thang điểm 10 (từ 0 đến 10), làm tròn đến 1 chữ số thập phân.

12. Phương pháp kiểm tra, đánh giá kết quả học tập

Sinh viên được đánh giá kết quả học tập trên cơ sở hai điểm thành phần như sau:

1. *Điểm đánh giá quá trình: trọng số 40% bao gồm:*

a. Điểm chuyên cần: 1, trọng số 10%

b. Điểm kiểm tra thường xuyên: 3, trọng số 30%

2. *Điểm thi kết thúc học phần: trọng số 60%*

Hình thức thi: Tiểu luận/ Bài tập lớn

Ma trận quan hệ giữa Chuẩn đầu ra và phương pháp kiểm tra, đánh giá

Hình thức đánh giá	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7	CLO8	CLO9	CLO10	CLO11
Tự luận	X	X	X	X	X	X	X	X	X	X	X
Dự lớp	X	X	X	X	X	X	X	X	X	X	X

13. Tài liệu phục vụ cho học phần (các tài liệu xuất bản trong 05 năm trở lại đây và cung cấp được cho Trung tâm Học liệu nơi đặt tài liệu)

13.1. Tài liệu chính

- Paco Hope and Ben Walther (2008). Web Security Testing Cookbook. O'REILLY, ISBN: 978-0-596-51483-9
- Dafydd Stuttard, Marcus Pinto (2011). The web application hacker's handbook. 2rd edition, Wiley publishing, Inc.

13.2. Tài liệu tham khảo

- William Stallings. (2011). "Network Security Essentials", 4th Edition. Prentice Hall, ISBN: 9780136108054.
- James F. Kurose, Keith W. Ross (2021). "Computer Networking: A Top-Down Approach" (https://gaia.cs.umass.edu/kurose_ross/online_lectures.htm)

TP.Hồ Chí Minh, ngày ... tháng ... năm 2024

Hiệu trưởng	Trưởng Bộ môn	Giảng viên biên soạn
Duyệt	(Ký và ghi rõ họ tên)	(Ký và ghi rõ họ tên)
		TS. Nguyễn Quang Tấn