ĐỀ CƯƠNG CHI TIẾT

QUẢN TRỊ VÀ BẢO MẬT WEBSITE

Mã học phần: - Số tín chỉ: 03

Dùng cho (các) ngành: **Công nghệ thông tin**

Điều kiện tiên quyết (nếu có): Mạng máy tính, Truyền số liệu

Hình thức đào tạo: Trực tiếp

Đơn vị phụ trách: Khoa Công nghệ thông tin

1. Mô tả chung về học phần

Quản trị và bảo mật Website là một dạng ứng dụng phổ biến và được triển khai rộng rãi nhất trong các tổ chức và doanh nghiệp. Sự phát triển bùng nổ của nó cũng kéo theo những tiềm ẩn đáng lo ngại trong vấn đề bảo mật. Các cuộc tấn công Website không chỉ tăng nhanh chóng về mặt số lượng mà các phương pháp tấn công cũng ngày càng tinh vi và có tổ chức. Học phần này nhằm cung cấp cho người học những kiến thức nền tảng cho bảo mật Website như các nguyên tắc bảo mật trong ứng dụng Web, một số lỗ hổng bảo mật Website phổ biến mà tin tặc có thể lợi dụng để khai thác, các kỹ thuật tấn công và giải pháp phòng chống.

2. Các chữ viết tắt (nếu có)

Từ viết tắt	Tiếng anh	Tiếng Việt

3. Chuẩn đầu ra của học phần

Mã	Chuẩn đầu ra học phần
plo10b	Vận dụng kỹ năng cài đặt, cấu hình, quản trị web
plo10c	Vận dụng kiến thức đã học để đảm bảo an toàn thông tin cho hệ thống thông tin và mạng máy tính ở doanh nghiệp
plo10d	Vận dụng bảo mật ứng dụng web

4. Giáo trình và tài liệu học tập

4.1. Giáo trình và tài liệu học tập:

Tập slide bài giảng

4.2. Tài liệu tham khảo:

[1]. Mike Shema, *Hacking Web Apps. 'Detecting rind Preventing Web Application Security Probleitis'*. Elsevier, 2012

[2]. Bryan Sullivan, Vincent Liu, *Web Application Secut' ity, A Deginner's Guide 1st Eclition.* McGiaw-Hill Education Group, 2011.

[3]. Dafydd Stuttai'd, Marcus Pinto, *T/tc Web Application Hacker's Hunclbook. Fishing and Exploiting $ecut 'iiy Flaws Paperback. IoY* Wiley & Sons, Inc, 2011.

5. Chiến lược học tập

Sinh viên cần tích cực và chủ động tham gia vào quá trình học tập; cần tham gia đầy đủ các giờ học theo quy định, không ngừng phấn đấu để duy trì sự tiến bộ liên tục trong học tập; hoàn thành nhiệm vụ học tập đúng tiến độ.

Để hoàn thành tốt học phần này, sinh viên cần:

- Tham gia đầy đủ các buổi học.
- Tập trung nghe giảng
- Chủ động đọc tài liệu và làm bài tập trước khi tham dự buổi học kế tiếp.
- Tích cực tham gia thảo luận; mạnh dạn đưa ra các ý tưởng, giải pháp, chính kiến của mình.
- Thực hành đầy đủ phòng lap

6. Nội dung, kế hoạch giảng dạy và đánh giá

Nội dung và kế hoạch giảng dạy, đánh giá	Hoạt động học tập của người học				Chuẩn đầu ra
	Trên lớp	ST	Tự học	SG	
Chương 1: Tổng quan về bảo mật ứng dụng Web 1.1. Giới thiệu về ứng dụng Web 1.2. Bảo mật ứng dụng Web 1.3. Quản trị và đánh giá an toàn 1.3.1. Phân loại tài sản 1.3.2. Phân tích mối đe dọa 1.3.3. Phân tích rủi ro 1.4. Quản trị bảo mật ứng dụng Web 1.4.1. Xác thực, ủy quyền 1.4.2. Bảo mật trình duyệt 1.4.3. Bảo mật CSDL 1.4.4. Bảo mật tin	- Nghe giảng - Thảo luận các vấn đề liên quan đến giám sát mạng: Đưa ra giải pháp của mình về các vấn đề được nêu ra trong quá trình thảo luận; Đặt các câu hỏi và tham gia thảo luận xung quanh nội dung bài học; Thể hiện quan điểm của mình về ý kiến của người khác.	5	- Ôn tập bài cũ - Cách đánh giá độ an toàn - Các nguyên tác bảo mật ứng dụng Web - Thực hành	10	plo10b
Chương 2: Các kỹ thuật tấn công và cách phòng chống 2.1. Kỹ thuật tấn công Cross – Site Seripting và cách phòng chống	- Nghe giảng - Thảo luận các vấn đề liên quan đến các kỹ thuật tấn công và đưa	25	- Ôn lại - Nghiên cứu trước và làm báo cáo các kỹ	40	plo10b plo10c

2.2. Kỹ thuật tấn công Cross – Site Request Forgery và cách phòng chống 2.3. Kỹ thuật tấn công Clickjacking và cách phòng chống 2.4. Kỹ thuật tấn công Injection và cách phòng chống 2.5. Kỹ thuật tấn công từ chối dịch vụ tầng ứng dụng	ra giải pháp phòng chống tấn công		thuật tấn công - Thực hành lập trình minh họa		
Chương 3: Chứng thực, Quản lý phiên làm việc và chống rò rỉ thông tin 3.1. Mật khẩu 3.2. Chứng thực đa yếu tố 3.3. Chứng thực và quản lý phiên làm việc 3.4. Đăng nhập một lần 3.5. Bảo mật ứng dụng Web chống rò rỉ thông tin, bảo mật tập tin thư mục.	- Nghe giảng - Thảo luận các vấn đề liên quan đến chứng thực, quản lý phiên làm việc và chống rò rỉ thông tin - Phân biện các cuộc tấc công chứng thực, giải pháp ngăn chặn - Làm bài tập nhóm một số chuyên đề	15	- Đọc trước tài liệu slide, chuẩn bị câu hỏi thảo luận. - Cài đặt công cụ thu thập các bản ghi nhật ký thiết bị để phân tích theo dõi.	30	plo10b plo10c plo10d
Tổng số tiết/giờ học		**45**			

ST: Số tiết chuẩn SG: Số giờ

7. Đánh giá kết quả học tập

Hoạt động đánh giá của học phần gồm:

Phân loại	**Phương pháp đánh giá**	**Tỷ trọng**	**Chuẩn đầu ra**		
			plo10b	**plo10c**	**plo10d**
Quá trình	ĐG1: Đánh giá thường xuyên trong suốt quá trình học	40%	x	x	x
	ĐG2: Kỹ năng cài đặt, cấu hình công cụ giám sát, áp dụng trong giám sát mạng.	30%		x	x
	ĐG3: Đánh giá khả năng vận dụng kiến thức đã học, phân tích, đề xuất giải pháp xây dựng hệ thống giải quyết các vấn đề của bài toán thực tế.	30%			x
	Tổng cộng:	100%			

7.1. Hoạt động đánh giá 1 - Chuẩn đầu ra: plo10b - Tỷ lệ: **40%** điểm học phần

- Hình thức đánh giá: Thường xuyên.
- Mô tả bài đánh giá:

- Hoạt động này được thực hiện thông qua bài thực hành và kiểm tra tại phòng máy nhằm đánh giá mức độ hiểu biết và kỹ năng cài đặt, cấu hình, quản trị web trên mạng
- Sinh sẽ được yêu cầu: Cài đặt cấu hình LAMP
  - Cài đặt Linux (Ubuntu server, Ubuntu Client), Apache Web server, My SQL, PHP
  - Cấu hình Apache và PHP
  - Cài đặt và cấu hình Firewall
  - Thiết lập mật khẩu bảo vệ thư mục Web trong Apache
- Sinh viên có thể tham gia đánh giá nhiều lần trong suốt quá trình học môn học. Kết quả sẽ trung bình cộng của các lần đánh giá.

- Ma trận đánh giá:

Tiêu chí đánh giá	**Khung điểm**				
	A	**B**	**C**	**D**	**F**
	8,5 ÷ 10	**7,0 ÷ 8,4**	**5,5 ÷ 6,9**	**4,0 ÷ 5,4**	**< 4,0**
(1) Mô tả và giải thích các vấn đề cơ bản trong quản trị hệ thống mạng. (70%).	Mô tả đúng, và giải thích được đầy đủ, chặt chẽ.	Mô tả đúng, và giải thích được nhưng chưa đầy đủ.	Mô tả đúng, nhưng chưa giải thích được.	Mô tả được nhưng vẫn còn một ít sai sót.	Mô tả có nhiều sai sót.
(2) Tham gia thảo luận, đề xuất giải pháp (30%).	Đưa ra được giải pháp đúng, hợp lý, giải thích thuyết phục	Đưa ra được giải pháp đúng, hợp lý, giải thích chưa hoàn toàn thuyết phục	Đưa ra được giải pháp đúng, chưa hoàn toàn hợp lý.	Giải pháp đưa ra chưa hoàn toàn đúng.	Giải pháp đưa ra sai.

Kết quả đánh giá chung:

Đánh giá 1 = **(1)*70% + (2) *30%** Tính theo thang điểm 10. Điểm cuối cùng sẽ được tính là trung bình cộng của các lần đánh giá.

7.2. Hoạt động đánh giá 2 - Chuẩn đầu ra: plo10c **-** Tỷ lệ: **30%** điểm học phần

- Hình thức đánh giá: đảm bảo an toàn thông tin cho mạng máy tính trên nền tảng web
- Mô tả bài đánh giá:
  - Hoạt động này được thực hiện thông qua bài thực hành và kiểm tra tại phòng máy nhằm đánh giá mức độ hiểu biết và kỹ năng cài đặt, cấu hình, quản trị web trên mạng .
  - Sinh viên sẽ được yêu cầu: Vận dụng hiểu được các kỹ thuật tấn công và chống tấn công, cài đặt và cấu hình các ứng dụng web, hiểu các dạng tấn công và đưa giải pháp phòng chống hiệu quả.

- Cài đặt ứng dụng DVWA (Damn Vulnerable Web App) để khai thác các lỗ hổng bảo mật ứng dụng Web
- Các dạng tấn công và phòng chống XSS
- Các dạng tấn công và phòng chống CSRF
- Các dạng tấn công và phòng chống SQL Injection
- Các dạng tấn công và phòng chống Command Injection
- Cài đặt và cấu hình Fai2ban để bảo vệ Apache khỏi các cuộc tấn công DDoS

  - Hoạt động đánh giá này được thực hiện ngay sau khi hoàn thành chương 2. Nếu chưa đạt, sinh viên được đánh giá lại ở tuần tiếp theo.

- Ma trận đánh giá:

Tiêu chí đánh giá	**Khung điểm**				
	A	**B**	**C**	**D**	**F**
	8,5 ÷ 10	**7,0 ÷ 8,4**	**5,5 ÷ 6,9**	**4,0 ÷ 5,4**	**< 4,0**
(1) Cài đặt và cấu hình công cụ giám sát mạng. (70%).	Cài đặt và cấu hình đúng; giải thích được đầy đủ, chặt chẽ; xử lý được các tình huống lỗi phát sinh	Cài đặt và cấu hình đúng; giải thích được đầy đủ, chặt chẽ; chưa xử lý được các tình huống lỗi phát sinh	Cài đặt và cấu hình đúng; giải thích chưa được đầy đủ, chặt chẽ.	Cài đặt và cấu hình đúng; chưa giải thích được.	Cài đặt và cấu hình chưa đúng.
(2) Tham gia thảo luận, đề xuất giải pháp áp dụng (30%).	Đưa ra được giải pháp đúng, hợp lý, giải thích thuyết phục	Đưa ra được giải pháp đúng, hợp lý, giải thích chưa hoàn toàn thuyết phục	Đưa ra được giải pháp đúng, chưa hoàn toàn hợp lý.	Giải pháp đưa ra chưa hoàn toàn đúng.	Giải pháp đưa ra sai.

Kết quả đánh giá chung:

Đánh giá 2 = (1)*70% + (2) *30% Tính theo thang điểm 10

7.3. Hoạt động đánh giá 3 - Chuẩn đầu ra: plo10d - Tỷ lệ: **30%** điểm học phần

- Hình thức đánh giá: Báo cáo bài tập lớn
- Mô tả bài đánh giá:
  - Hoạt động này được thực hiện thông qua đánh giá dưới hình thức bảo vệ bài tập lớn, nhằm đánh giá khả năng vận dụng các kiến thức đã được thu nhận của môn học để xây dựng hệ thống giải quyết vấn đề của bài toán thực tế.
  - Sinh viên sẽ được yêu cầu: Hiểu vận dụng được bảo mật ứng dụng web
    - Cài đặt và cấu hình SSL và HTTPS cho Apache Web server
    - Tạo chứng chỉ số SSL và cấu hình Apache để sử dụng chứng chỉ SSL
    - Cài đặt cấu hình tường lửa ứng dụng Web
    - Thiết lập các qui tắc (rule)
    - Thiết lập bảo mật ứng dụng Web chống rò rỉ thông tin

- Thời điểm và cách thức công bố kết quả đánh giá: Hoạt động đánh giá này được
  thực hiện sau khi kết thúc học phần chương 3. Nếu chưa đạt, sinh viên được đánh giá lại sau khi báo cáo 01 tuần.

- Ma trận đánh giá:

Tiêu chí đánh giá	**Khung điểm**				
	A	**B**	**C**	**D**	**F**
	8,5 ÷ 10	**7,0 ÷ 8,4**	**5,5 ÷ 6,9**	**4,0 ÷ 5,4**	**< 4,0**
(1)Cài đặt, phân tích các yêu cầu của bài toán và đề xuất lựa chọn giải pháp (60%).	Cài đặt, phân tích các yêu cầu của bài toán rõ ràng, các giải pháp được lựa chọn là phù hợp, giải thích chặt chẽ.	Cài đặt, phân tích các yêu cầu của bài toán rõ ràng, các giải pháp được lựa chọn là phù hợp nhưng giải thích chưa đầy đủ.	Cài đặt, phân tích các yêu cầu của bài toán rõ ràng, các giải pháp đề ra chưa hoàn toàn thích hợp,	Cài đặt, phân tích các yêu cầu của được bài toán nhưng chưa rõ ràng	Không phát biểu, phân tích được các yêu cầu bài toán.
(2) Triển khai các giải pháp bảo mật ứng dụng Web chống rò rỉ thông tin. (40%).	Triển khai các giải pháp giám sát phù hợp với yêu cầu; giải thích đầy đủ chặt chẽ; xử lý được các tình huống lỗi phát sinh.	Triển khai các giải pháp giám sát phù hợp với yêu cầu; giải thích đầy đủ chặt chẽ; chưa xử lý được các tình huống lỗi phát sinh.	Triển khai các giải pháp giám sát phù hợp với yêu cầu; giải thích chưa được đầy đủ, chặt chẽ.	Triển khai các giải pháp giám sát phù hợp với yêu cầu; chưa giải thích được.	Triển khai các giải pháp giám sát nhưng chưa phù hợp với yêu cầu.

Kết quả đánh giá chung:

Đánh giá 3 = (1)*60% + (2) *40% Tính theo thang điểm 10

7.4. Cách tính kết quả học tập chung của học phần

Điểm học phần = Đánh giá 1 × 40% + Đánh giá 2 × 30% + Đánh giá 3 × 30%

8. Các phương tiện, trang thiết bị dạy và học

- Giảng đường, máy chiếu, phòng thực hành.
- Yêu cầu đối với sinh viên: Có tài liệu môn học, máy tính PC hoặc Laptop.

9. An toàn của sinh viên và giảng viên

- Giảng viên, sinh viên phải đọc kỹ và tuân thủ nghiêm túc nội quy phòng học và phòng thực hành. Đọc kỹ và chấp hành đúng các quy định về việc sử dụng các trang thiết bị điện tại phòng học, phòng thực hành.
- Trong trường hợp phát sinh các vấn đề có thể dẫn đến mất an toàn, sinh viên cần kịp thời báo cáo với giảng viên để phối hợp giải quyết.

10. Kỷ luật, khiếu nại và hỗ trợ

- Sinh viên phải có mặt trên lớp đủ thời gian theo quy định của nhà trường
- Gian lận trong hoạt động đánh giá nào sẽ hủy kết quả đánh giá đó.
- Sinh viên có quyền khiếu nại trực tiếp giảng viên về kết quả đánh giá ngay sau khi kết quả được công bố kết quả.
- Sinh viên gặp bất kỳ khó khăn gì trong học tập học phần này có thể liên hệ trực tiếp với giảng viên, Chủ nhiệm khoa/bộ môn, Văn phòng hỗ trợ sinh viên, Phòng Đào tạo và Ban Thanh tra đào tạo của Nhà trường để được hướng dẫn và hỗ trợ.

Chủ tịch Hội đồng **xây dựng CTĐT ngành**	*Hải Phòng, ngày tháng năm 2022* **Người biên soạn**
	
	Nguyễn Trọng Thể