Trường Đại học Bách Khoa - ĐHQG Tp.HCM
Khoa: Khoa Khoa học và Kỹ thuật Máy tính
Khoa/Bộ môn quản lý MH: Công nghệ Phần mềm

Tp.HCM, ngày ..... tháng ..... năm .....

Đề cương môn học Sau đại học

BẢO MẬT PHẦN MỀM
(SOFTWARE SECURITY)

Mã số MH: CO5250

Số tín chỉ:	**Tc (LT.BT&TH.Tự Học): 3**						**ECTS: 6**				
Số tiết -Tổng:	**75**	LT:	**30**	BT:	**0**	TH:	**0**	ĐA:		BTL/TL:	**45**
Đánh giá:	Bài tập:			30%							
	Thuyết trình:			20%							
	Cuối kì:			50%							
- Môn tiên quyết:											
- Môn học trước:											
- Môn song hành:											
- CTĐT ngành (Mã ngành):	Khoa Học Máy Tính (8480101)										
- Ghi chú khác:											

1. <u>Mục tiêu môn học:</u>

Môn học này cung cấp các kỹ thuật bảo mật phần mềm ứng dụng trong việc xây dựng các phần mềm an toàn. Môn học cũng giới thiệu các nguyên lý của việc thiết kế, phát triển, và kiểm thử tính an toàn của các hệ thống phần mềm.

Aims:

This course teaches software engineering techniques for building security into software as it is developed. Also, it introduces students to the discipline of designing, developing, and testing secure and dependable software-based systems. Students will be exposed to the techniques needed for the practice of effective software security techniques.

2. <u>Nội dung tóm tắt môn học:</u>

Môn học này giới thiệu cho sinh viên các nguyên lý của việc thiết kế, phát triển và kiểm thử tính an toàn của các hệ thống phần mềm. Sinh viên sẽ nhận được các kiến thức nền tảng về quản lý rủi ro, kiểm thử tính an toàn tại các mức như white box, balck box, ... Sinh viên còn được cung cấp các kiến thức về kĩ thuật coding an toàn và khả năng thiết kế, kiểm tra các yêu cầu bảo mật.

Course outline:

Software Security introduces students to the discipline of designing, developing, and testing secure and dependable software-based systems. Studens will get fundametal knowledge of risk management, security

testing at basic levels such as white box, black box, ... Students are also provided knowledge as Secure coding techniques, and how to design, valid, and verify security requirements.

3. Tài liệu học tập:

[1] Mathias Payer: Software Security Principles, Policies, and Protection, HexHive Books, 2019

[2] Ross Anderson: Security Engineering, 2nd Edition, Wiley, 2008

[3] Mark Dowd, John McDonald, Justin Schuh: The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities, Addison Wesley, 2006

[4] Robert Hansen, Jeremiah Grossma: Clickjacking, SecTheory, 2008

[5] Gary McGraw, Brian Chess, Sammy Migues: Software [In]security: Software Security Top 10 Surprises, InformIT, 2008

4. Các hiểu biết, các kỹ năng cần đạt được sau khi học môn học:

STT	Chuẩn đầu ra môn học (CĐRMH)	Công cụ đánh giá CĐRMH	Đóng góp CĐR Chương trình (CĐRCT)		
			Ứng dụng	Nghiên cứu	
CĐRMH.1	Khả năng nắm bắt các khái niệm và kĩ thuật trong an ninh phần mềm	Thuyết trình, Cuối kì	h, i		1.3
CĐRMH.2	Khả năng áp dụng các kiến thúc nền tảng vào giải quyết bài toán thực tế	Bài tập	i		2.1
CĐRMH.3	Khả năng hiểu các kĩ thuật code an toàn và chống lại các mối nguy cơ phổ biến trong phát triển phần mềm	Thuyết trình, Cuối kì	i, j		1.4, 2.1

Learning outcomes:

No.	Course learning outcomes (CLO)	CLO assessment	Matching with PLO		
			Coursework	Research	
L.O.1	Ability to have fundermental knowledge of software security	Report, Final exam	h, i		1.3
L.O.2	Ability to apply basic knowledge in solving real case studies	Exercises	i		2.1
L.O.3	Understanding secure coding practices to prevent common vulnerabilities from being injected into software.	Report, Final exam	i, j		1.4, 2.1

Bảng ánh xạ chuẩn đầu ra môn học và chuẩn đầu ra chương trình ứng dụng:

	Chuẩn đầu ra của chương trình (CĐRCT)										
Chuẩn đầu ra môn học (CĐRMH)	a	b	c	d	e	f	g	h	i	j	k
CĐRMH.1								✓	✓		
CĐRMH.2									✓		
CĐRMH.3									✓	✓	

Bảng ánh xạ chuẩn đầu ra môn học và chuẩn đầu ra chương trình nghiên cứu:

	Chuẩn đầu ra của chương trình (CĐRCT)										
Chuẩn đầu ra môn học (CĐRMH)	a	b	c	d	e	f	g	h	i	j	k
CĐRMH.1											

	Chuẩn đầu ra của chương trình (CĐRCT)										
Chuẩn đầu ra môn học (CĐRMH)	a	b	c	d	e	f	g	h	i	j	k
CĐRMH.2											
CĐRMH.3											

5. Hướng dẫn cách học - chi tiết cách đánh giá môn học:

Phương pháp học chủ yếu sẽ là nghe các bài giảng, tham gia thảo luận trên lớp và nghiên cứu các trường hợp điển hình.

Học viên nên có một vai trò tích cực trong môn học, cần tham dự đầy đủ các bài giảng và tham gia tích cực vào việc thảo luận, trình bày trên lớp.

Học viên sẽ phải hoàn thành các bài tập về nhà, đồ án môn học, chuyên đề, bài tập lớn và làm một bài thi cuối kỳ.

Cách đánh giá:

- Bài tập: 30%

- Thuyết trình môn học: 20%

- Thi cuối kì: 50%

Learning strategies & Assessment Scheme:

The primary learning method will be attending lectures, participating in class discussions and studying case studies.
Students should have an active role in the courses, should attend all lectures, be actively involved in discussion and give presentation in class.
Students will be required to complete homework, assignments, projects, and take the final examination.

Grading:
- Exercies: 30%
- Project: 20%
- Final exam: 50%

6. Nội dung chi tiết:

Tuần/ Buổi	Chủ đề (chương)	Nội dung	Chuẩn đầu ra môn học	Tài liệu
1	Giới thiệu	- Giới thiệu- Định nghĩa các thuật ngữ- Security Development Lifecycle		Sách [1,2]
2	OWASP	- OWASP: Nguy cơ an toàn ứng dụng- Case studies		Sách [1]Internet
3	Các lỗ hổng thiết kế trong phần mềm	- Các lỗi thiết kế- Case studies		Sách [1,2]Internet
4	Các nguyên lý thiết kế	- Các nguyên lý trong thiết kế phần mềm- Case studies		Sách [1]
5	Chính sách bảo mật và Quyền riêng tư	- Chính sách bảo mật- Chính sách quyền riêng tư		Sách [2]
6	Mô hình mối nguy cơ	- Định nghĩa- Các mối nguy cơ- Mô hình		Sách [1,2]

Tuần/ Buổi	Chủ đề (chương)	Nội dung	Chuẩn đầu ra môn học	Tài liệu
7	Yêu cầu bảo mật	- Định nghĩa- Yêu cầu- Case studies		Sách [1]
8	Static Analysis, Dynamic Analysis, and Fuzzing	- Các khái niệm- Các kĩ thuật phân tích- Case studies		Sách [1,2]
9	Chu trình phát triển phần mềm an toàn	- Các khái niệm- Chu trình phần mềm- Bài tập		Sách[1,2]
10	Security Testing	- Khái niệm- Kiểm thử phần mềm- Bài tập		Sách [1,2]

7. <u>Giảng viên tham gia giảng dạy:</u>

CBGD chính:	TS. Trương Tuấn Anh
CBGD tham gia:	TS. Lê Lam Sơn

XÁC NHẬN
CỦA HỘI
ĐỒNG XÂY
DỰNG
CHƯƠNG
TRÌNH ĐÀO
TẠO VÀ KHOA

Tp. Hồ Chí Minh, ngày ..... tháng ..... năm .....

GIẢNG
VIÊN
LẬP ĐỀ
CƯƠNG

TS. Phạm
Hoàng
Anh