

TRƯỜNG ĐẠI HỌC VĂN LANG
ĐƠN VỊ: KHOA CÔNG NGHỆ THÔNG TIN

ĐỀ THI/ĐỀ BÀI, RUBRIC VÀ THANG ĐIỂM
THI KẾT THÚC HỌC PHẦN
Học kỳ 1, năm học 2024-2025

I. Thông tin chung

Tên học phần:	An ninh Ứng dụng Web		
Mã học phần:	71ITNW40703	Số tín chỉ:	3
Mã nhóm lớp học phần:	241_71ITNW40703_01		
Hình thức thi: Đề án	Thời gian làm bài:		Phút/ ngày
☐ Cá nhân	☒ Nhóm		
<i>Quy cách đặt tên file</i>	<i>Mã SV_Ho va ten SV_Mã đề tài</i>		

II. Các yêu cầu của đề thi nhằm đáp ứng CLO

(Phần này phải phối hợp với thông tin từ đề cương chi tiết của học phần)

Ký hiệu CLO	Nội dung CLO	Hình thức đánh giá	Trọng số CLO trong thành phần đánh giá (%)	Câu hỏi thi số	Điểm số tối đa	Lấy dữ liệu đo lường mức đạt PLO/PI
(1)	(2)	(3)	(4)	(5)	(6)	(7)
CLO1	Phát triển mô hình bảo mật vào việc xây dựng an ninh ứng dụng web theo yêu cầu doanh nghiệp	Đề án	50%	Các yêu cầu về nội dung của CSLT, thực nghiệm của đề tài	5	PLO2/P I 2.1
CLO3	Thực hiện trách nhiệm cá nhân vào việc thực hiện đề án nhóm và giải quyết các vấn đề liên quan đến nhóm	Đề án	50%	Personal, Khả năng trình bày, Trả lời câu hỏi	5	PL07/PI 7.1
			100%		10	

III. Nội dung đề bài

1. Đề bài

Mã đề tài	Tên Đề tài	Cơ sở lý thuyết	Thực nghiệm
WAS-01	Phát hiện lỗ hổng Cross-site scripting với XSSStrike	- Lỗ hổng XSS: Reflected, stored, DOM-base - Tấn công XSS trong thực tế - Tìm và khai thác lỗ hổng XSS - Phòng chống tấn công XSS - Công cụ XSSStrike	- Môi trường kiểm thử: Mô hình, mô tả mô hình - Mục tiêu - Kịch bản, các bước thực hiện - Hoàn thành được tấn công, phòng chống Reflected, stored, DOM-base - Sử dụng XSSStrike trên Kali Linux, tạo web kiểm thử trên Linux OS
WAS-02	Triển khai tấn công vào các cơ chế xác thực trên ứng dụng web	- Tấn công vào các cơ chế xác thực (Chương 6, trang 119) - Công cụ (Metasploit, Hydra, ZAP)	- Môi trường kiểm thử: Mô hình, mô tả mô hình - Mục tiêu - Kịch bản, các bước thực hiện - Hoàn thành được tấn công, phòng chống 3 điểm yếu trong cơ chế xác thực (Design Flaws in Authentication Mechanisms) - Sử dụng các công cụ trên Kali Linux, tạo web kiểm thử trên Linux OS
WAS-03	Khai thác lỗ hổng SQL Injection trên ứng dụng web sử dụng Microsoft SQL Server với Sqlninja	- Injecting into SQL (trang 291) - Công cụ Sqlninja	- Môi trường kiểm thử: Mô hình, mô tả mô hình - Mục tiêu - Kịch bản, các bước thực hiện - Hoàn thành được tấn công, phòng chống In-band SQL Injection, Blind SQL Injection, Out-of-band SQL Injection - Sử dụng Sqlninja trên Kali Linux, tạo web kiểm thử trên Linux OS

WAS-04	Tự động hóa quá trình phát hiện và khai thác các lỗ hổng SQL injection với sqlmap	- Injecting into SQL (trang 291) - Công cụ Sqlninja	- Môi trường kiểm thử: Mô hình, mô tả mô hình - Mục tiêu - Kịch bản, các bước thực hiện - Hoàn thành được tấn công, phòng chống In-band SQL Injection, Blind SQL Injection, Out-of-band SQL Injection - Sử dụng sqlmap trên Kali Linux, tạo web kiểm thử trên Linux OS
WAS-05	Lỗ hổng A10:2021 – Server-Side Request Forgery	https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/	- Môi trường kiểm thử: Mô hình, mô tả mô hình - Mục tiêu - Kịch bản, các bước thực hiện - Hoàn thành 3 trong 4 kịch bản do OWASP đề xuất
WAS-06	Lỗ hổng A01:2021 – Broken Access Control	https://owasp.org/Top10/A01_2021-Broken_Access_Control/	- Môi trường kiểm thử: Mô hình, mô tả mô hình - Mục tiêu - Kịch bản, các bước thực hiện - Hoàn thành 2 kịch bản do OWASP đề xuất
WAS-07	Lỗ hổng A07:2021 – Identification and Authentication Failures	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/	- Môi trường kiểm thử: Mô hình, mô tả mô hình - Mục tiêu - Kịch bản, các bước thực hiện - Hoàn thành 3 kịch bản do OWASP đề xuất

2. Hướng dẫn thể thức trình bày đề bài

Đề án được viết bằng TIẾNG VIỆT bao gồm những vấn đề được trình bày theo trình tự sau:

- (1) Trang bìa (Theo mẫu)
- (2) Mục lục
- (3) Nội dung

Nội dung đề án Trình bày theo yêu cầu và hướng dẫn của giảng viên dựa trên tính chất của từng đề tài mà sinh viên thực hiện. Có thể chia làm 2 chương:

- Chương 1: CƠ SỞ LÝ THUYẾT
- Chương 2: THỰC NGHIỆM

- (4) Tài liệu tham khảo (Danh mục các loại tài liệu tham khảo, bao gồm: các loại tài liệu, giáo trình, bài giảng hoặc tài liệu tham khảo từ mạng Internet sinh viên phải chỉ rõ nguồn gốc của tài liệu đã sưu tầm)

Hình thức trình bày: ngắn gọn, rõ ràng, mạch lạc, sạch sẽ, không được tẩy xóa, có đánh số trang, đánh số bảng biểu, hình vẽ.

3. Rubric và thang điểm

Tiêu chí	Trọng số (%)	Tốt Từ 8-10đ	Khá Từ 6 – dưới 8đ	Trung bình Từ 4 – dưới 6đ	Yếu Dưới 4đ
Mô tả đồ án và cơ sở lý thuyết	10%	Mô tả đồ án và cơ sở lý thuyết đầy đủ, súc tích, rõ ràng và thực tiễn, thể hiện được ứng dụng cho doanh nghiệp	Mô tả đồ án và cơ sở lý thuyết đầy đủ nhưng cách trình bày chưa súc tích	Mô tả đồ án và cơ sở lý thuyết không đủ nội dung	Mô tả đồ án và cơ sở lý thuyết sai hướng đề tài
Mô hình, mục tiêu, kịch bản	10%	- Mô hình IP, logic được thiết kế đúng. - Mục tiêu, kịch bản chuyên nghiệp, chính xác, có tính thực tiễn.	- Mô hình IP, logic được thiết kế đúng. - Mục tiêu, kịch bản tạm ổn	- Mô hình IP, logic được thiết kế đúng. - Mục tiêu, kịch bản còn thiếu nhiều nội dung	Mô hình IP, logic, mục tiêu, kịch bản chưa chính xác theo đề tài đặt ra
Triển khai thực nghiệm	30%	- Thực hiện chính xác, chuyên nghiệp việc triển khai thực nghiệm. - Phân tích và triển khai được các giải pháp phòng vệ	- Thực hiện chính xác việc triển khai thực nghiệm. - Phân tích và đề xuất được các giải pháp phòng vệ	- Thực hiện chính xác việc triển khai thực nghiệm. - Chưa phân tích và chưa đề xuất được các giải pháp phòng vệ	Không hoàn thành được triển khai thực nghiệm
Personal	20%	Cá nhân được cả nhóm đánh giá tốt	Cá nhân được cả nhóm đánh giá đóng góp chỉ 75% dự án	Cá nhân được cả nhóm đánh giá đóng	Cá nhân được cả nhóm đánh giá

				góp chỉ 50% dự án	đóng góp 0% dự án
Khả năng trình bày	20%	Nói rõ, tự tin, thuyết phục, giao lưu người nghe	Nói rõ, tự tin, giao lưu người nghe	Không rõ lời, thiếu tự tin, ít giao lưu người nghe	Nói nhỏ, không tự tin, không giao lưu người nghe
Trả lời câu hỏi	10%	Trả lời đúng tất cả các câu hỏi và có mở rộng và phát triển câu trả lời để giải quyết vấn đề	Trả lời chính xác 70-80% tổng số câu hỏi	Trả lời chính xác 50-69% tổng số câu hỏi	Trả lời không chính xác trên 50% tổng số câu hỏi
Tổng	100				

TP. Hồ Chí Minh, ngày tháng năm 2024

Người duyệt đề

Giảng viên ra đề

Ths. Trần Quang Nhật

ThS. Bùi Duy Cường