VIETNAM NATIONAL UNIVERSITY – HO CHI MINH CITY

UNIVERSITY OF INFORMATION TECHNOLOGY

SYLLABUS

NT213 – WEB AND APPLICATION SECURITY

1. GENERAL INFORMATION

Course name (Vietnamese):	**Bảo mật web và ứng dụng**
Course name (English):	**Web and Application Security**
Code:	**NT213**
Type of course:	Specialization
Deparment:	Faculty of Computer Networks and Communications
Instructor:	MSc. Đỗ Hoàng Hiển, MSc. Phan Thế Duy MSc. Đỗ Thị Thu Hiền Email: hiendh@uit.edu.vn
Number of credits:	3
Theory:	2
Lab:	1
Self-study:	
Prerequisite course(s):	
Pre-course(s):	NT208 - Web technology and applications

2. COURSE DESCRIPTION

This course aims to provide students with fundamental skills and knowledge of:

- Analyzing and identifying threats, vulnerabilities, and weaknesses of web and mobile applications.
- Basic skills of exploiting vulnerabilities on web and applications.
- Securely developing applications and deploying systems.
- Ensuring confidentiality and integrity of data.

3. COURSE GOALS

Table 1.

Goal No.	Goal description	Program outcomes	Level (Bloom)
G1	Describe security issues on applications and systems	*LO2 (2.7.4, 2.7.6)*	*Knowledge - 3*
G2	Identity and search threats, vulnerabilities, and weaknesses of web and mobile applications, and exploit common vulnerabilities existing on the applications	*LO3 (3.1, 3.2)*	*Skill - 4*
G3	Propose security solutions for applications, and develop applications and build systems securely	*LO3 (3.3), LO4 (4.1)*	*Skill - 4*

4. COURSE LEARNING OUTCOMES

Table 2.

Course outcomes	Descriptions	Level of teaching
G1.1	Understand operations and configurations of applications and systems	*I*
G1.2	Describe security issues on web and applications	*I, T*
G2.1	Identity and search threats, vulnerabilities, and weaknesses of web and mobile applications	*I, T*
G2.2	Analyze and exploit common vulnerabilities existing on the applications	*I, T, U*
G3.1	Propose security solutions for applications and data, focusing on web and mobile applications	*I, T*
G3.2	Develop applications and build systems securely	*I, T, U*

(I – Introduce, T – Teach, U – Utilize)

5. COURSE CONTENT, LESSON PLAN

a. Theory

Table 3.

Week (X hours)	Contents	Course learning outcomes	Activities	Assessment element
1+2 (4 class hours)	**Chapter 1: Operations and configurations of web applications and systems** 1.1 Introduce to operations of web application architecture and programming languages 1.2 Operations and configurations of SQL and NoSQL 1.3 Operations and configurations web servers and Linux	G1.1	**Group formation.** **Teaching:** Lecturer gives structions, demo, questions. **Study in class:** Exchange related issues, problems. **Study at home:** Do homework.	*A1, A2, A3*
3 (2 class hours)	**Chapter 2: OWASP Top Ten Web Application Security Risks** 2.1 OWASP tools and burp suite 2.2 OWASP Cheat sheets 2.3 OWASP Top 10 Web Application Security Risks **Assign the projects to the groups**	G1.1, G1.2, G2.1	**Group allocation.** **Teaching:** Lecturer gives structions, demo, question. **Study in class:** Discuss the projects. **Study at home:** Do homework.	*A1, A3*
4 (2 class hours)	**Chapter 3: Cross-Site Request Forgery and Cross Site Scripting** 3.1 Cross-Site Request Forgery 3.1.1. Overview 3.1.2. Attack scenarios 3.1.3. Countermeasures 3.2 Cross Site Scripting 3.2.1. Overview 3.2.2. Attack scenarios 3.2.3. Countermeasures	G1.2, G2.1, G2.2, G3.1	**Group allocation.** **Teaching:** Lecturer gives structions, demo, questions. **Study in class:** Exchange related issues, problems, Practice on the vulnerable web applications. **Study at home:**	*A1, A2, A3*

			Do homework.	
5 (2 class hours)	**Chapter 4: SQL Injection** 4.1 Overview 4.2 Risk Factors 4.3 Classify 4.4 Attack scenarios 4.5 Countermeasures	G1.2, G2.1, G2.2, G3.1	**Teaching:** Lecturer gives structions, demo, questions. **Study in class:** Exchange related issues, problems, Practice on the vulnerable web applications. **Study at home:** Do homework.	*A1, A2, A3*
6 (2 class hours)	**Chapter 5: File Inclusion and Command Injection** 5.1 File Inclusion 5.1.1. Overview 5.1.2. Classify 5.1.3. Attack scenarios 5.1.4. Countermeasures 5.2 Command Injection 5.2.1. Overview 5.2.2. Attack scenarios 5.2.3. Countermeasures	G1.2, G2.1, G2.2, G3.1	**Teaching:** Lecturer gives structions, demo, questions. **Study in class:** Exchange related issues, problems, Practice on the vulnerable web applications. **Study at home:** Do homework.	*A1, A3*
7 (2 class hours)	**Chapter 6: WAF bypass techniques** 6.1 Motivation & Objective 6.2 Introduction to Web Application Firewall (WAF) 6.3 Bypassing SQL Injection Filters 6.4 Bypassing XSS Filters 6.5 Bypassing Command Injection Filter	G1.2, G2.1, G2.2	**Teaching:** Lecturer gives structions, demo, questions. **Study in class:** Exchange related issues, problems. **Study at home:** Research bypassing techniques for other filters.	*A1, A2, A3*

8 (2 class hours)	**Chapter 7: Anatomy of Mobile** 7.1 Mobile App Technology Stacks 7.2 AndroidOverview 7.3 Android Application Development	G1.1	**Teaching:** Lecturer gives structions, demo, questions. **Study in class:** Exchange related issues, problems.	*A2, A3*
9+10 (4 class hours)	**Chapter 8: Android Security** 8.1 Android Security Model 8.1.1. Application Sandboxing 8.1.2. Permissions 8.1.3. Inter-Process Communication 8.1.4. Code Signing & Platform Key 8.2 Data protection on Android devices 8.3 Secure application connections to servers 8.4 OWASP Mobile Top 10	G1.2, G2.1, G2.2, G3.1	**Teaching:** Lecturer gives structions, questions. **Study in class:** Exchange related issues, problems. **Study at home:** Do homework.	*A1, A2, A3*
11 (2 class hours)	**Chapter 9: Hacking and Penetration testing** 9.1 Ethical Hacking 9.1.1. Overview 9.1.2. Hacking Phases 9.1.3. Common Vulnerabilities and Exposures 9.2 Penetration Testing 9.2.1. Overview 9.2.2. Classify 9.2.3. Report	G1.2, G2.1	**Teaching:** Lecturer gives structions, questions. **Study in class:** Exchange related issues, problems.	*A1, A3*
12-15	**Students present their project results.**	G2.2, G3.1	Students report their projects. Lecturer gives comments on projects and has	*A1*

			quiz for students of each group.	

b. Lab

Table 4.

Week (5 class hours per week)	Contents	Course learning outcomes	Activities	Assessment element
1	**Lab 1**: **Basic Web Application Programming** ● HTML and JavaScript ● PHP and Database ● HTML Form	G2.2	**Teaching:** Lecturer provides environment, describes the objective of the lab and gives instructions for students. **Study in class:** Students follow the instruction of the lab. **Self-study:** Students read the instruction and prepare the lab at home.	*A2*
2	**Lab 2: Cross Site Scripting and Cross-Site Request Forgery** ● Cross-site scripting attack and prevention ● Cross-Site Request Forgery attack and prevention	G2.1, G2.2, G3.1	**Teaching:** Lecturer provides environment, describes the objective of the lab and gives instructions for students. **Study in class:** Students follow the instruction of the lab. **Self-study:** Students read the instruction and prepare the lab at home.	*A2*
3	**Lab 3: SQL Injection** ● SQL Injection attack ● SQL Injection prevention with	G2.1, G2.2, G3.1	**Teaching:** Lecturer provides environment, describes the objective of the lab and gives instructions for students. **Study in class:** Students follow the instruction of the lab.	*A2*

	Prepared Statement		**Self-study:** Students read the instruction and prepare the lab at home.	
4	**Lab 4**: **Basic Android Application Programming** ● Android components ● Activity lifecycle ● Basic Android GUI application	G2.2	**Teaching:** Lecturer describes the objective of the lab and gives instructions for students. **Study in class:** Students follow the instruction of the lab. **Self-study:** Students read the instruction and prepare the lab environment at home.	*A2*
5	**Lab 5**: **Android security** ● Mobile Security Framework ● Static Code Analysis ● Exploiting basic vulnerabilities	G2.1, G2.2, G3.1	**Teaching:** lecturer describes the objective of the lab and gives instructions for students. **Study in class:** Students follow the instruction of the lab. **Self-study:** Students read the instruction and prepare the lab environment at home.	*A2*
6	**Lab 6: Basic WAF bypass techniques** ● Bypassing filters	G2.1, G2.2	**Teaching:** Lecturer provides environment, describes the objective of the lab and gives instructions for students. **Study in class:** Students follow the instruction of the lab. **Self-study:** Students read the instruction and prepare the lab at home.	*A2*

6. COURSE ASSESSMENT

Table 5.

Assessment element	Course learning outcomes	Percentage (%)
A1. Progress assessment	*G1.1, G1.2, G2.1, G2.2*	*20%*

A1.1 In-class exercise /homework/quiz/ CTF challenges A1.2 Course project	*G3.1, G3.2*	*10%* *20%*
A2. Mid-term exam		*0%*
A3. Lab	*G2.1, G2.2, G3.1*	*30%*
A4. Final exam	*G1.1, G1.2, G2.1, G2.2, G3.1*	*40%*

a. Assessment A1

The lecturer assigns various types of exercises and CTF challenges for students to evaluate the outcome G1.1, G1.2, G2.1, G2.2.

No.	Assessment type	Percentage (%)	Scale	Marking/Rubric
1	Programming/ Analyzing source code	5%	10	Web and Android programming Analyzing source code, identifying/searching vulnerabilities and weakness
2	CTF challenges	5%	10	Working on virtual laboratory, online CTF challenges (automatic grading)
3	Project	20%	10	Criteria 1: Report (1/10) Criteria 2: Theory background (3/10) Criteria 2: Demo (4/10) Criteria 3: Q&A (2/10)

b. Assessment A2

The practice test score is the average of 6 practice sessions, each practice has a marking guide.

c. Assessment A3

The final exam includes (but is not limited to)

- Multiple choice questions: 30 - 40 question for G1.1, G1.2, G2.1.
- Written: 2-3 questions for G2,2, G3.1.

7. COURSE REQUIREMENTS AND EXPECTATIONS

- **Laboratory**: labs can be done in group in laboratories. Lecturer describes the objective of the labs and gives instructions for students. Students must fulfill all lecturer's requirements. Late submission is not accepted.
- **Projects**: lecturers hand out team-work projects for the students. Late submission is not accepted.
- **Class attendance**: Students are checked their attendance in class by in-class. Failing to show up by the time of checking is considered to be absent.
- **Final examination**: Students that fail to show up on the examination day without acceptable reasons will get 0.

8. COURSE MATERIALS

1. Bryan Sullivan, Vincent Liu, "Web Application Security, A Beginner's Guide", McGraw-Hill, 2011.
2. Mike Shema, "Hacking Web Apps: Detecting and Preventing Web Application Security Problems", Syngress Publishing, 2012.
3. Michal Zalewski, "The Tangled Web: A Guide to Securing Modern Web Applications", William Pollocky, 2012.
4. Jeff Six, "Application Security for the Android Platform", O'Reilly Media, 2011.

Reference

1. Welcome to the OWASP Top 10 – 2021: https://owasp.org/Top10/ (last access 03/01/2022)
2. OWASP Cheat Sheet Series: https://cheatsheetseries.owasp.org/ (last access 03/01/2022)
3. OWASP Mobile Top 10: https://owasp.org/www-project-mobile-top-10/ (last access 03/01/2022)

9. SOFTWARE, TOOLS

1. OWASP® Zed Attack Proxy (ZAP): https://www.zaproxy.org/ (last access 03/01/2022)
2. OWASP Broken Web Applications: https://owasp.org/www-project-broken-web-applications/ (last access 03/01/2022)
3. OWASP Juice Shop: https://owasp.org/www-project-juice-shop/ (last access 03/01/2022)
4. Burp Suite: https://portswigger.net/burp (last access 03/01/2022)
5. Android Studio: https://developer.android.com/studio (last access 03/01/2022)

Faculty Head **Date: Month, Date, Year**

Instructor