AN TOÀN ỨNG DỤNG WEB VÀ CƠ SỞ DỮ LIỆU
(WEB APPLICATION AND DATABASE SECURITY)
Đề cương chi tiết (Course Syllabus)

1. General Information

Course name: An toàn ứng dụng web và cơ sở dữ liệu (Web Application and Database Security)

Course code: SEC1408_CLC

Course type: Compulsory

Number of credits: 3

2. Objectives

Knowledge:

The aim of this course is to provide students with advanced knowledge of web and database security, including security requirements, web vulnerabilities and attacks, security solutions for servers, applications, and browsers, database security models, attack techniques, security mechanisms, backup, recovery, auditing, and monitoring.

Skills:

On successful completion of this course a student will be able to:

- Analyze security threats, weaknesses, and vulnerabilities in web applications and databases.
- Select and implement appropriate security measures to protect web applications and databases.

Attitude:

Students are required to attend the classes and complete assignments/projects.

3. Abstracts

This course provides students with advanced knowledge of web applications and database security, including security requirements for web applications and databases, threats, weaknesses, and vulnerabilities in web applications, security approaches, types of web application attacks, and security measures for servers, applications, and browsers. The course also covers database security models, common attack techniques on databases, database security mechanisms, and security considerations in web development and deployment. Additionally, it includes topics on backup, recovery, auditing, and monitoring of database operations.

4. Teaching and learning methods

Lectures: 24 hours
Exercises: 3 hours
Projects : 10 hours
Labs: 8 hours

5. Prerequisites:

- Required: Fundamentals of Information Security - SEC1401_CLC
- Prior Courses: Database - INT1313_CLC, Computer Networks - INT1336_CLC

6. Learning outcomes

After completing this course, the student is able to:
[CLO1]: Explain fundamental concepts in web and database security
[CLO2]: Evaluate appropriate security solutions for web and database security issues
[CLO3]: Implement security solutions for web applications and databases

7. Assignment criteria

Learning outcomes	Assignment criteria
[CLO1]: Explain fundamental concepts in web and database security	Chapter 1, Chapter 2, Chapter 3, Chapter 4, Chapter 5, Chapter 6, Chapter 7
[CLO2]: Evaluate appropriate security solutions for web and database security issues	Chapter 2, Chapter 3, Chapter 4, Chapter 6, Chapter 7
[CLO3]: Implement security solutions for web applications and databases	Chapter 2, Chapter 3, Chapter 4, Chapter 7

8. Outlines

Chapter 1: Overview of Web Application Security
1.1 Introduction to Web Services and Web Application Architecture
1.2 Security Threats and Vulnerabilities in Web Applications
1.3 Principles of Web Application Security
1.4 Approaches to Web Application Security

Chapter 2: Common Attacks on Web Applications
2.1 HTML Injection and Cross-Site Scripting (XSS)
2.2 Cross-Site Request Forgery (CSRF)
2.3 SQL Injection Attacks
2.4 Attacks on Authentication Mechanisms
2.5 Exploiting Design Flaws
2.6 Attacks on Web Browsers and User Privacy
2.7 Case Studies on Web Application Vulnerabilities and Attacks

Chapter 3: Security Measures for Servers, Applications, and Web Browsers
3.1 Web Server Security
3.2 Web Application Security
3.3 Web Browser Security

Chapter 4: Security in Web Application Development and Deployment
4.1 Approaches to Secure Web Application Development and Deployment
4.2 Models and Methods for Secure Software Development

Chapter 5: Overview of Database Security

5.1 General Concepts
5.2 Database Security Requirements
5.3 General Security Models and Security Layers in Databases
5.4 Common Database Attack Techniques

Chapter 6: Database Security Mechanisms

6.1 Authentication and Authorization in Databases
6.2 Object Security in Databases
6.3 Encryption in Databases
6.4 Other Database Security Measures
6.5 Security Models in Database Management Systems
6.6 Security Auditing and Evaluation of Database Systems

Chapter 7: Database Backup, Recovery, Auditing, and Monitoring

7.1 Backup and Recovery Strategies
7.2 Database Auditing
7.3 Monitoring Database Server Activities

9. Required Textbooks

[1] Bryan Sullivan, Vincent Liu, *Web Application Security: A Beginner's Guide*, McGraw-Hill, 2012.
[2] Alfred Basta, Melissa Zgola, *Database Security*, Cengage Learning, 2012.

10. Suggested Textbooks

[3] Hoang Xuan Dau, *Lecture Notes on Web Application and Database Security*, PTIT, 2021.
[4] Mike Shema, *Hacking Web Apps: Detecting and Preventing Web Application Security Problems*, Elsevier Inc., 2012.

11. Schedule

Main contents	Duration	Specific contents
Chapter 1: Overview of Web Application Security	2h lecture	1.1 Introduction to Web Services and Web Application Architecture 1.2 Security Threats and Vulnerabilities in Web Applications 1.3 Principles of Web Application Security 1.4 Approaches to Web Application Security
Chapter 2: Common Attacks on Web Applications	6h lecture 1h excercise	2.1 HTML Injection and Cross-Site Scripting (XSS) 2.2 Cross-Site Request Forgery (CSRF) 2.3 SQL Injection Attacks 2.4 Attacks on Authentication Mechanisms 2.5 Exploiting Design Flaws

		2.6 Attacks on Web Browsers and User Privacy 2.7 Case Studies on Web Application Vulnerabilities and Attacks
Chapter 3: Security Measures for Servers, Applications, and Web Browsers	4h lecture 1h excercise 4h lab	3.1 Web Server Security 3.2 Web Application Security 3.3 Web Browser Security
Chapter 4: Security in Web Application Development and Deployment	2h lecture 10h project	4.1 Approaches to Secure Web Application Development and Deployment 4.2 Models and Methods for Secure Software Development
Chapter 5: Overview of Database Security	2h lecture 1h excercise	5.1 General Concepts 5.2 Database Security Requirements 5.3 General Security Models and Security Layers in Databases 5.4 Common Database Attack Techniques
Chapter 6: Database Security Mechanisms	4h lecture 2h lab	6.1 Authentication and Authorization in Databases 6.2 Object Security in Databases 6.3 Encryption in Databases 6.4 Other Database Security Measures 6.5 Security Models in Database Management Systems 6.6 Security Auditing and Evaluation of Database Systems
Chapter 7: Database Backup, Recovery, Auditing, and Monitoring	4h lecture 2h lab	7.1 Backup and Recovery Strategies 7.2 Database Auditing 7.3 Monitoring Database Server Activities

12. Grading Policy

Attendance:	10%
Mid-term exam/exercises:	10%
Course projects:	30%
Final examination:	50%