Course Specifications

Course Title:	**Web Security**
Course Code:	**CSEC 417**
Program:	**Information and Computer Science**
Department:	**Computer Science and Information**
College:	**Science**
Institution:	**Majmaah University**

Table of Contents

A. Course Identification

1. Credit hours:3	

2. Course type

a.   University ☐   College ☐   Department ☐   Others ☐

b.   Required ☐   Elective ▣

3. Level/year at which this course is offered: Selective

4. Pre-requisites for this course (if any)**:**
ICS 322 & CSEC 323

5. Co-requisites for this course (if any)**:**

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	48	80%
2	**Blended**	6	10%
3	**E-learning**	6	10%
4	**Correspondence**	0	0%
5	**Other**	0	0%

7. Actual Learning Hours (based on academic semester)

No	Activity	Learning Hours
Contact Hours		
1	**Lecture**	30
2	**Laboratory/Studio**	0
3	**Tutorial**	30
4	**Others** (specify)	0
	Total	60
Other Learning Hours*		
1	**Study**	45
2	**Assignments**	15
3	**Library**	10
4	**Projects/Research Essays/Theses**	10
5	**Others** (specify)	0
	Total	80

* The length of time that a learner takes to complete learning activities that lead to achievement of course learning outcomes, such as study time, homework assignments, projects, preparing presentations, library times

B. Course Objectives and Learning Outcomes

1. Course Description

This course is a comprehensive overview of web security. The goal is to build an understanding of the most common web attacks and their countermeasures. Given the pervasive insecurity of the modern web landscape, there is a pressing need for programmers and system designers to improve their understanding of web security issues. The course will be covering the fundamentals as well as the state-of-the-art in web security. Topics include principles of web security, attacks and countermeasures, the browser security model, web app vulnerabilities, injection, denial-of-service, TLS attacks, privacy, fingerprinting, same-origin policy, cross site scripting, authentication, JavaScript security, emerging threats, defense-in-depth, and techniques for writing secure code.

2. Course Main Objective

1. Get hands-on experience on web programming
2. Critically audit web applications for security flaws.
3. Design and implement exploits for real security bugs.
4. Develop secure web applications.

3. Course Learning Outcomes

	CLOs	Aligned PLOs
1	**Knowledge:**	
1.1	be familiar with protocols and specifications for secure communication: WWW and Web Services security (SSL, SET)	K3-CS
1.2	E-mail security (PGP)	K3-CS
2	**Skills :**	
2.1	be able to create keys and sign certificate	S3-CS
2.2	be able to encipher and decipher an arbitrary file	S3-CS
3	**Competence:**	
3.1	be familiar with different threats and attacks on application level	C3-CS
3.2	actively participate in discussions about firewalls and database security	C3-CS

C. Course Content

No	List of Topics	Contact Hours
1	Web Basics: HTML, CSS, JS, URLs, DOM, Frames, HTTP, Navigation, X-Domain communication	4
2	Network Attacks & HTTPS	4
3	Limitations of HTTPS	4
4	Same Origin Policy & Web Attacker Model Injection Flaws (I): Cross-site Scripting (XSS)	8
5	Injection Flaws (II) : XSS (contd.), SQL Injection, OS Command Injection, HTTP Header Injection	8
6	(I) Authentication Flaws (II) Request Authorization Flaws	8
7	Insecure Web Logic: Logic Flaws, HTTP Pollution, HTTP Parameter Tampering	8
8	Cookie Flaws and Server Misconfiguration	4
9	Attacks on User Interfaces	4
10	Browser Design & Flaws	4

11	User Privacy: Browser & Device Fingerprinting, User Tracking, Browser Caching Flaws	4
	Total	60

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge**		
1.1	be familiar with protocols and specifications for secure communication: WWW and Web Services security (SSL, SET)	Lectures Lab demonstrations Case studies Individual presentations	Written Exam Homework assignments Lab assignments Class Activities Quizzes
1.2	E-mail security (PGP)		
2.0	**Skills**		
2.1	be able to create keys and sign certificate	Lectures Lab demonstrations Case studies Individual presentations Brainstorming	Written Exam Homework assignments Lab assignments Class Activities Quizzes Observations
2.2	be able to encipher and decipher an arbitrary file		
3.0	**Competence**		
3.1	be familiar with different threats and attacks on application level	Small group discussion Whole group discussion Brainstorming Presentation	Observations Homework assignments Lab assignments Class Activities
3.2	actively participate in discussions about firewalls and database security		

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	First written mid-term exam	6	15%
2	Second written mid-term exam	12	15%
3	Presentation, class activities, and group discussion	Every week	10%
4	Homework assignments	After each chapter	10%
5	Implementation of presented algorithms	Every two weeks	10%
6	Final written exam	16	40%
7	Total		100%
8			

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice. (include amount of time teaching staff are expected to be available each week)

- 5-office hours per week in the lecturer schedule.
- The contact with students by e-mail, mobile, office telephone, website and BlackBoard.

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	Andrew Hoffman, Web Application Security, O'Reilly Media, Inc., March 2020, ISBN: 9781492053118.
Essential References Materials	Peter Yaworski, Real-World Bug Hunting: A Field Guide to Web Hacking, July 2019.
Electronic Materials	Video lectures are available for students at the time of the course.
Other Learning Materials	https://systemoverlord.com/2020/07/10/comparing-3-great-web-security-books.html

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom and Labe available at College of science in Zulfi.
Technology Resources (AV, data show, Smart Board, software, etc.)	All resource are available in the halls
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	N\A

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment	Students Reviewers	Questionnaires (course evaluation) filled by the students and electronically organized by the university. Student-faculty and management meetings.

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Quality of learning resources	Program Leaders	Direct/indirect

Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	