

Course Syllabus

1.	Course title	Security of Web Applications
2.	Course number	1911351
3.	Credit hours (theory, practical)	3
	Contact hours (theory, practical)	3
4.	Prerequisites/corequisites	Web Applications Development (1904120) and Introduction to Database Systems (1902224)
5.	Program title	Cybersecurity
6.	Year of study and semester (s)	Third year
7.	Final Qualification	Bachelor degree
8.	Other department (s) involved in teaching the course	None
9.	Language of Instruction	English
10.	Date of production/revision	February 26, 2023
11.	Required/ Elective	Required

12. Course Coordinator:

Dr. Khair Eddin Sabri

Office numbers: KASIT 117

Office hours:

Monday: 11:30 – 12:30

Tuesday, Thursday: 11:30 – 12:30

Phone number: 22557

Email addresses: k.sabri@ju.edu.jo

13. Other instructors:

14. Course Description:

This course introduces students to a foundation in the theories and practice relating to web application security. Topics covered: web applications vulnerabilities and attacks, building secure web applications, concepts associated with deploying and securing a typical HTTP environment as well as defensive techniques that can be employed. Teaching of this course will be based on active learning methodology such that students will work in groups to discuss and analyze the vulnerability in web applications.

15. Course aims and outcomes:

A- Aims:

Goal:

The main goal of this course is to provide student with the knowledge and skills to develop a secure web application.

Objectives:

- *Understand the main threats on web applications.*
- *Develop a secure web application.*

B- Intended Learning Outcomes (ILOs): Upon successful completion of this course students will be able to ...

A-Knowledge and understanding: with the ability to ...

- A1) Understand the main security properties*
- A2) Understand client side attacks*
- A3) Understand backend attacks.*
- A4) Understand the main techniques of authentication*
- A5) Understand The different techniques of SQL injection attack*
- A6) Understand the different techniques of XSS attacks*
- A7) Understand the main ethics related to web security*

B- Intellectual skills: with the ability to ...

- B1) Distinguish between reflected, stored, and DOM XSS attacks*
- B2) Distinguish between different types of SQL injection attacks*
- B3) Identify the places that could be vulnerable to CSRF attack*
- B4) Identify the main vulnerability related to access control*
- B5) Identify the main client side attacks*
- B6) Identify the main backend attacks*

C- Subject specific skills – with ability to ...

- C1) Analyze the security of a web application as blackbox*
- C2) Analyze the security of a web application as whitebox.*
- C3) Develop a secure web application.*

D- Transferable skills – with ability to

- D1) Work in group to analyze and design web applications.*

16. Topic Outline and Schedule:

Topic	Week	ILOs	Student Outcomes	TLA (teaching, learning and Assessment)
Information to Web Application Security and ethics	1	A1, A7	4, 6	T: Lectures and discussion L: Resources A: Lab, Project, Midterm, Final
Client Side Control	2	A2	2, 6	T: Lectures and discussion L: Resources

				A: Lab, Project, Midterm, Final
Authentication	3	A3, A4, B6, C1, C2, C3, D1	1, 2, 6	T: Lectures and discussion L: Resources A: Lab, Project, Midterm, Final
Access Control	4	A3, A4, B4, B6, C1, C2, C3, D1	1, 2, 6	T: Lectures and discussion L: Resources A: Lab, Project, Midterm, Final
SQL Injection Attack	5	A3, A5, B2, B6, C1, C2, C3, D1	2, 6	T: Lectures and discussion L: Resources A: Lab, Project, Midterm, Final
Directory Traversal and OS Command Injections Attacks	6	A3, B6, C1, C2	2, 6	T: Lectures and discussion L: Resources A: Lab, Project, Midterm, Final
Information Disclosure	7	A3, B6, C1, C2, C3, D1	2, 6	T: Lectures and discussion L: Resources A: Lab, Project, Midterm, Final
File upload and SSRF	8	A3, B6, C1, C2, C3, D1	2, 6	T: Lectures and discussion L: Resources A: Lab, Project, Final
Midterm	9			
XXE	10	A3, B6, C1, C2	2, 6	T: Lectures and discussion L: Resources A: Lab, Project, Final
XSS injection attack	11	A2, A6, B1, B5, C1, C2, C3, D1	2, 6	T: Lectures and discussion L: Resources A: Lab, Project, Final
CORS policy	12	A2, B5, C1, C2	1, 2, 6	T: Lectures and discussion L: Resources A: Lab, Project, Final
CSRF attack	13	A2, B3, B5, C1, C2, C3, D1	2, 6	T: Lectures and discussion L: Resources A: Lab, Project, Final
Other topics such as OAuth, JWT	14	A2, A3, B5, C1, C2	2, 6	T: Lectures and discussion L: Resources A: Lab, Project, Final
Revision	15			
Final	16			

17. Evaluation Methods and Course Requirements (Optional):

Opportunities to demonstrate achievement of the ILOs are provided through the following assessment methods and requirements:

There will be several assessment methods of evaluation the performance of the students: For each topic the student is required to solve at least three labs which will be given and discussed in the class. Students are required to develop a secure web application. Students will be required to analyze applications as blackbox and whitebox.

18. Course Policies:

A- Attendance policies:

Deliberate abstention from attending 1911351 classes and any other similar acts will lead to student deprivation from the course according to the UJ regulations

B- Absences from exams and handing in assignments on time:

If you miss the midterm, then a makeup exam will not be provided unless you submit a valid absence excuse, within three days from the midterm, to your lecturer. This excuse must be signed and stamped from the UJ hospital in order to be valid. If your lecturer accepts the excuse, then you will be able to take the makeup. You need to follow up the departmental announcements regarding the makeup date and time. Please note that the lecturer may either accept or reject your excuse based on UJ regulations

C- Health and safety procedures:

N/A

D- Honesty policy regarding cheating, plagiarism, misbehavior:

All students in this course must read the University policies on plagiarism and academic honesty

http://registration.ju.edu.jo/RegRegulations/Forms/All_Regulations.aspx

E- Grading policy:

- Midterm Exam:	30%
- Labs and Project:	20%
- Final Exam:	50%

F- Available university services that support achievement in the course:

N/A

G- Statement on Students with disabilities

Students with Disabilities: Students with disabilities who need special accommodations for this class are encouraged to meet with the instructor and/or their academic advisor as soon as possible. In order to receive accommodations for academic work in this course, students must inform the course instructor and/or their academic advisor, preferably in a written format, about their needs no later than the 4th week of classes.

19. Required equipment:

20. References:

A- There is not textbook for the courses. The following resources can be used

1. *Web Security Academy. Portswigger.net*
2. *Web Security for Developers. Real Threats, Practical Defense, Malcolm McDonald, William Pollock, 2020.*

3. *Web Application Security, A Beginner's Guide, Bryan Sullivan and Vincent Liu, McGraw Hill, 2012*
4. *Web Application Security Exploitation and Countermeasures for Modern Web Applications, Andrew Hoffman, O'Reilly, 2020.*

21. Additional information:

Course website:
elearning.ju.edu.jo

Date: -----

Name of Course Coordinator: Dr. Khair Eddin Sabri Signature: -----

Head of curriculum committee/Department: ----- Signature: -----

Head of Department: ----- Signature: -----

Head of curriculum committee/Faculty: ----- Signature: -----

Dean: ----- Signature: -----

Copy to:

Head of Department

Assistant Dean for Quality Assurance

Course File