

**Department of Business Information Technology (BIT)**

**King Abdullah II School for IT**

**The University of Jordan**

**M S C . W E B I N T E L L I G N E N C E**

**Course Name: Web Applications Security (1904710)**

---

Instructor name: Dr. Ja'far Alqatawna \_\_\_\_\_

Office number: \_\_\_\_\_

Office hours: \_\_\_\_\_

E-mail address: J.Alqatawna@ju.edu.jo \_\_\_\_\_

**Course Description:**

Web applications security, as branch of secure software design, focuses on how to design and develop dependable and trustworthy web applications. Having completed this course the student will be able to participate in, and cooperate with, web application development teams with a goal to achieving appropriate levels of security for web products. It introduces students to Saltzer and Schroeder security design principles and how security can be integrated with the web application development lifecycle. The course covers common web vulnerabilities such as Cross-Site Scripting, Cross-site Request Forgery, SQL injection and more. Topics such as threat modeling, abuse cases and secure programming will be discussed as well.

**Course Objectives:**

Having completed this course the student will be able to participate in, and cooperate with, web application development teams with a goal to achieving appropriate levels of security for that team's software products. It aims to:

- Develop a working knowledge of security design principles.
- Develop an understanding of common software vulnerabilities - Web in particular- and how to avoid them.
- Develop a working knowledge of how security can be integrated with the web application development lifecycle.
- Develop a working knowledge of techniques, tools, methodologies and standards to evaluate software security.
- Provide understanding of the trade-off between security and other system's properties such as usability and availability.

**Learning Outcomes:**

Upon successful completion of this course, students will be able to:

- Identify common Web vulnerabilities, their causes, symptoms, and remedies.
- Understand the roles and activities in project management that promote secure software development.
- Apply secure software design principles, methods and tools for the secure implementation of those designs.
- Apply suitable security architectures.
- Relate to standards of relevance for the area of secure software engineering, in particular to understand the advantages, roles, mechanisms, and difficulties involved in methods for evaluating assurance in security of software.

## Recommended reading materials

**Software Security: Building Security In**, McGraw (2006).

**Beginning ASP.NET Security**, Barry Dorrans. Wiley (2010).

**Top 10 Most Critical Web Application Security Risks**, OWASP (2013).

**Web Penetration Testing with Kali Linux**, Muniz & Lakhani, Packet (2013)

**Mastering the Certified Secure Software Lifecycle Professional**, Krutz & Fry (2009).

**Building Secure Software: How to Avoid Security Problems the Right Way.**  
Viega & McGraw. Addison-Wesley (2001).

**Fundamental Practices for Secure Software development.** A Guide to the Most Effective Secure Development Practices in Use Today (2008).

**A Guide to Building Secure Web Applications and Web Services.** The Open Web Application Security Project (OWASP), 2005.

Selected papers covering related topics will be provided to students during the course.

<b>Week</b>	<b>Topic</b>
<b>1</b>	Preliminary concepts and terminologies
<b>2</b>	Introduction to software security
<b>3</b>	Security design principles and secure programming techniques.
<b>4</b>	Software vulnerabilities, their causes and symptoms
<b>5</b>	Secure SDLC and other secure S.E. methodologies.
<b>6</b>	Web application security.
<b>7</b>	Web Security requirement analysis, abuse cases and threat modeling.
	Midterm Exam
<b>8</b>	Security Auditing, related tools and standards.
<b>9</b>	Improper use of cryptography and Random Number Generators
<b>10</b>	Security vs. functionality and usability
<b>11</b>	Layered security and defense in depth
	Paper presentations
<b>15</b>	<b>Final Exam</b>

**Grading:**

The total grades of this course are assigned as follows

- |                                  |      |
|----------------------------------|------|
| 1. 2 Hour exam                   | 30%  |
| 2. Final Exam                    | 40%  |
| 3. Class Participations and HWs  | 10%  |
| 4. Research paper & presentation | 20 % |

**Attendance**

Students are expected to attend class; there is no system of permitted absences. The instructor in each class determines the effect of absences on a student's grade in that class." Students may not normally receive credit for a course if they do not attend the class meetings.

**Project and term paper:**

Each Student is expected to participate in several tasks covering various topics in web and secure software development. Each student will also submit and present a term paper that forms a basis for a publishable research paper.

**GOOD LUCK!**