Course Title	Web Applications Security				
Course Code	WSS554				
Course Type	Specialization (Elective)				
Level	Master (2nd Cycle)				
Year / Semester	2 or 3				
Teacher's Name	Christiana Ioannou				
ECTS	10	Lectures / week	3	Laboratories/week	0
Course Purpose	The purpose of the course is to provide the students the knowledge of the security concepts and principles underlying the field of web application. It touches a wide range of topics including the Web application structure and their vulnerabilities, the attacks that are most prominent, and security measures to prevent the attack and its ramifications.				
Learning Outcomes	By the end of the course, the students are expected to: • be able to perform a series of zero-touch reconnaissance and information gathering and analyse information for web applications including their structure; • understand and identify web application vulnerabilities and weak points; • know the web application attacks and their effects; • critically evaluate the potential security measures to prevent attacks; • know the secure application techniques for enabling authentication and authorization.				
Prerequisites	None	Co-requisites	None		
Course Content	• **Web Application Information gathering:** Web Application Reconnaissance (Information gathering, Web application mapping), Structure of Web Applications (DOM, REST API, JavaScripts, Authentication and Authorization Systems, Web Servers, Server-Side Databases, Client-Side Data Stores), Finding Subdomains (Applications per Domain, Browser Network Analysis Tools, Search Engine Caches, Archives, Social Snapshots), Attacks (Zone Transfer Attacks, Brute Force Subdomains, Dictionary Attacks), API Analysis (Endpoint Discovery, Authentication Mechanisms), Weak Points in application architecture (Multiple Layers of Security) • **Attacks / Offense**: Hackers (mindset), Cross-Site Scripting (XSS Discovery and Exploitation), Cross-Site Request Forgery (CSRF Query Parameter Tampering, GET Payloads), XML External Entity (Direct/Indirect), Injection (SQL, Code, Command Injection), DoS-Denial of Service (regex DoS, Logical DoS Vulnerabilities, DDoS), Third party vulnerabilities. • **Security Defense:** Securing Web Applications (Vulnerability Discovery, Analysis and Management, Apply offense techniques), Secure				

	Application Architecture (Authentication and Authorization SSL/TLS, Secure Credentials), Defending Against Attacks (XSS, CSRF, XXE, Injection, DoS), Securing Third-Party Dependencies.
Teaching Methodology	The course is designed to introduce and explain the material students are expected to learn through lectures (3 hours per week) in classrooms or lectures theatres, by means of traditional tools or using computer demonstration. Lecture notes and presentations are available through the web (e-learning platform) for students to use in combination with the textbooks. Furthermore, theoretical principles are explained by means of specific examples and for solving specific problems using practical examples. Students are also advised to use the subject's textbook or reference books for further reading and practice. Auditory exercises, where examples regarding matter represented at the lectures, are solved and further, questions related to particular open-ended topic issues are compiled by the students and answered, during the lecture or assigned as homework. Furthermore, group projects are assigned to the students, where literature search is encouraged to identify a specific problem related to some issue, gather relevant scientific information about how others have addressed the problem, design and implement a solution as well as report the final solution in written and orally, via a presentation. Moreover, a number of case study readings are also considered to illustrate that what students have studied in each chapter is not just of academic or theoretical value but also has value in terms of improving real-life challenges.
Bibliography	The following textbooks are associated with topics considered at various points throughout this course. • W. Stallings, ***Network Security Essentials: Applications and Standards***, Pearson, 6th Ed., 2017 • Andrew Hoffman, **Web Application Security**, O'Reilly Media, Inc., 1st Ed., 2020 The above textbooks are recommended as sources of additional reading for students so as to elaborate on the course's material. Students can also find additional examples that they can use for practice. Other textbooks that explain security breach techniques will be used as reference: • Bryan Sullivan and Vincent Liu, ***Web Application Security, A Beginner's Guide***, McGraw Hill Professional, 1st Ed., 2011 Furthermore, students will be encouraged to explore other online / print sources that are related to topics covered in this course and may reference to new attacks in Web Applications.
Assessment	The Students are assessed via continuous assessment throughout the duration of the Semester, which forms the Coursework grade and the final

	written exam. The coursework and the final exam grades are weighted 50% and 50%, respectively, and compose the final grade of the course. Various approaches are used for the continuous assessment of the students, such as class participation and laboratory work, group project design, implementation and presentation. The assessment weight, date and time of each type of continuous assessment is being set at the beginning of the semester via the course outline. An indicative weighted continuous assessment of the course is shown below: • **Participation Activities** (10% of total marks for module) • **One marked (group) project** (30% of total marks for module) • **Presentation of group project** (10% of total marks for module) • **One closed-book, 3-hour exam** (50% of total marks for module) Students are prepared for final exam, by revision on the matter taught, problem solving and concept testing and are also trained to be able to deal with time constrains and revision timetable. The criteria considered for the assessment of each type of the continuous assessment and the final exam of the course are: (i) the comprehension of the fundamental concepts and theory of each topic, (ii) the application of the theory in solving related problems and (iii) the ability to apply the above knowledge in complex real-life problems. • The final assessment of the students is formative and summative and is assured to comply with the subject's expected learning outcomes and the quality of the course.
Language	English