Course Title	**Web Applications Security**				
Course Code	**DLWSS554**				
Course Type	**Elective**				
Level	Master (2nd Cycle) – Distance Learning				
Year / Semester	2 / 3				
Teacher's Name	**Christiana Ioannou, PhD**				
ECTS	10	Lectures / week	3	Laboratories/week	-
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		Co-requisites	None		
Course Content	This course consists of the following three (4) units that will be taught within twelve (12) weeks: • Unit 1 (Week 1): • Unit 2 (Weeks 2-5) deals with web application information gathering • Unit 3 (Weeks 6-8) introduces major attacks in web applications and the vulnerabilities they exploit • Unit 4 (Weeks 9-12) provides security measures to be used to prevent attacks from occurring. The details of the material to be taught for each unit are shown below **Unit 1: 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) **Unit 2: 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. **Unit 3: 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	**Mode of Delivery: Distance Learning** The course is designed to introduce and explain the material students are expected to learn through an on-line learning environment. The on-line environment provides an opportunity for receiving on-line feedback from the Course Instructor during their study. In addition, students will be encouraged to interact both with other students and the instructor so as to feel part of an on-line community of learners that belong to the University network. The course content will be delivered through online material/notes, recorded lectures and/or narrated presentations. Therefore, students may be asked to download and study notes, tutorials and numerical exercises as well as watch recorded lectures/demonstrations or narrated presentations posted on the web addressing the main concepts of a particular unit. Furthermore, the planned communication and the dynamic/online interaction activities between the course instructor and the students will include asynchronous communication tools (Discussion Forum) that students may be asked to participate, wherever appropriate, in an online forum posting their views on certain topics covered in a particular unit; and synchronous communication tools (instant messaging, such as Skype, chat rooms, video-conferencing, etc.), that students may discuss on-line with the Instructor (s) and/or other students specific issues covered in a given unit. Moreover, a number of case study readings are also considered to illustrate that what students have studied in each unit is not just of academic or theoretical.
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 dynamic online activities, online quizzes, 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: • **An online quiz** (15% of total marks for module) • **One marked assignment/project** (15% of total marks for module) • **Presentation of project** (10% of total marks for module) • **Two dynamic interactive activities** (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