Teaching Guide				
Identifying Data				2021/22
Subject (*)	Applications Security		Code	614530005
Study programme	Máster Universitario en Ciberseguridade			
Descriptors				
Cycle	Period	Year	Type	Credits
Official Master's Degree	1st four-month period	First	Obligatory	6
Language	Spanish			
Teaching method	Face-to-face			
Prerequisites				
Department	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicacións			
Coordinador	Bellas Permuy, Fernando	E-mail	fernando.bellas@udc.es	
Lecturers	Bellas Permuy, Fernando Losada Perez, Jose	E-mail	fernando.bellas@udc.es jose.losada@udc.es	
Web	moovi.uvigo.gal			
General description	Developing secure applications is not an easy task. Knowledge of the vulnerabilities that usually affect applications, the techniques of authentication, authorization and access control, as well as the incorporation of security into the development life cycle, is essential to be able to build and maintain applications successfully. In this course, all these aspects are studied in a practical way, with special emphasis on the development of web applications and services.			

Contingency plan	1. Modifications to the contents No changes. 2. Methodologies * Teaching methodologies that are maintained - Guest lecture / keynote speech. If any student cannot attend theory classes, due to partial confinement or capacity problems, university video conferencing systems will be used, integrated with the online synchronous teaching systems. In the event of a confinement situation that prevents theory classes from being taught in person, they will be taught synchronously at the official timetable through the university online teaching systems and will be recorded and put them available. - ICT practicals. In general, the same solution as for theory classes will be used. If lab classes need to be taught through the university online teaching systems, only general explanations will be recorded, since it is the only content that makes sense to record. There will no changes to lab projects, since they are developed in the student?s personal computer by using freely available software. - Multiple-choice questions. If it is not possible to do the test in person, it will be replaced by an online test. * Teaching methodologies that are modified None. 3. Mechanisms for personalized attention to students - Moodle. All teaching resources (slides, examples, lab project specification, notifications, etc.) will be available at Moodle. If theory or lab classes must be taught online, videos will be put available at Moodle. - University online teaching systems. If necessary, they will be used to teach theory and lab classes as commented above. Personal attention will be preferably by the same media. - E-mail. To any questions. 4. Modifications in the evaluation No changes. * Evaluation observations: No changes. 5. Modifications to the bibliography or webgraphy No changes are necessary. All bibliographic resources are public websites.

Study programme competences	
Code	Study programme competences
A2	CE2 - Deep knowledge of cyberattack and cyberdefense techniques

A7	CE7 - To demonstrate ability for doing the security audit of systems, equipment, the risk analysis related to security weaknesses, and for developing de procedures for certification of secure systems
A13	CE13 - Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks
B2	CB2 - Students will be able to apply their knowledge and their problem-solving ability in new or less familiar situations, within a broader context (or in multi-discipline contexts) related to their field of specialization
B7	CG2 - Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information, network or system security
C4	CT4 - Ability to ponder the importance of information security in the economic progress of society

Learning outcomes			
Learning outcomes	Study programme competences		
To know the vulnerabilities that applications usually suffer (with special emphasis on web applications and services) and prevention mechanisms.	AJ2 AJ7 AJ13	BJ2 BJ7	CJ4
To know the techniques of authentication, authorization and access control in applications and services.	AJ2 AJ7 AJ13	BJ2 BJ7	CJ4

Contents	
Topic	Sub-topic
Topic 1. Introduction.	1.1 Authentication, authorization and access control. 1.2 Stateful applications and services. 1.3 Stateless applications and services. 1.4 Server-side and SPA web applications.
Topic 2. Vulnerabilities and prevention mechanisms in applications and services.	2.1 Reference frameworks. 2.2 Vulnerabilities in the processing of input data. 2.3 Vulnerabilities in authentication. 2.4 Vulnerabilities in session management. 2.5 Sensitive data exposure. 2.6 Vulnerabilities in access control. 2.7 Incorrect configuration. 2.8 Monitoring and insufficient logging. 2.9 Vulnerabilities in third-party libraries.
Topic 3. Secure software development life cycles.	3.1 Security from the analysis phase. 3.2 Code revisions. 3.3 SAST and DAST tools.
Topic 4. Authentication, authorization and access control.	4.1 Introduction. 4.2 Authentication and authorization. 4.2.1 HTTP authentication. 4.2.2 JSON Web Token. 4.2.3 OAuth2. 4.2.4 OpenID Connect. 4.2.5 Other standards. 4.3 Access control. 4.3.1 Role-based access control (RBAC). 4.3.2 Attribute-based access control (ABAC).

Planning

Methodologies / tests	Competencies	Ordinary class hours	Student?s personal work hours	Total hours
Guest lecture / keynote speech	A2 A7 A13 B2 B7 C4	22.5	22.5	45
ICT practicals	A2 A7 A13 B2 B7 C4	19.5	73.5	93
Multiple-choice questions	A2 A7 A13 B2 B7 C4	2	8	10
Personalized attention		2	0	2
(*)The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.				

Methodologies	
Methodologies	Description
Guest lecture / keynote speech	Lessons taught by the teacher through the projection of slides. Lessons have a totally practical approach, explaining the theoretical concepts through the use of simple examples and case studies. Slides are available on the e-learning platform of the university.
ICT practicals	To experiment with the concepts studied in the course, students will perform two projects. The first one will be focused on the vulnerability analysis of a web application. Students will start from the source code of a web application and will have to detect the vulnerabilities, exploit them and fix them. The second project will be focused on authentication, authorization and access control. Students will start from the source code of an application, composed of a user interface and a service, and will have to implement authentication, authorization and access control, by following different strategies.
Multiple-choice questions	There will be a test to verify students have assimilated concepts correctly. The test will consist of a set of questions with several possible answers, being only one of them correct. Unanswered questions do not score, and wrong answers score negatively.

Personalized attention	
Methodologies	Description
ICT practicals	Tutorials and questions by email and Teams for specific doubts. Presence of the teacher in the lab to assist students in the development of lab projects.

Assessment			
Methodologies	Competencies	Description	**Qualification**
ICT practicals	A2 A7 A13 B2 B7 C4	Completion of the two projects is mandatory.	60
Multiple-choice questions	A2 A7 A13 B2 B7 C4	There will be a test to verify students have assimilated concepts correctly.	40

Assessment comments
To pass the course, it is necessary to obtain: 4 points at least (out of 10) in the evaluation of each project.4 points at least (out of 10) in the test.5 points at least (out of 10) in the final mark, which is calculated as follows: 0.60 * (0.70 * project1 + 0.30 * project2) + 0.40 * exam.Marks from projects and the test are saved from the first to the second call.

Sources of information

Basic	Open Web Application Security Project (OWASP), https://www.owasp.org.Common Weakness Enumeration (CWE), https://cwe.mitre.org.Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org.National Vulnerability Database (NVD), https://nvd.nist.gov.Common Attack Pattern Enumeration and Classification (CAPEC), https://capec.mitre.org.JSON Web Token (JWT), https://jwt.io.OAuth 2.0, https://oauth.net/2/.OpenID Connect, http://openid.net/connect/.Open Web Application Security Project (OWASP), https://www.owasp.org.Common Weakness Enumeration (CWE), https://cwe.mitre.org.Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org.National Vulnerability Database (NVD), https://nvd.nist.gov.Common Attack Pattern Enumeration and Classification (CAPEC), https://capec.mitre.org.JSON Web Token (JWT), https://jwt.io.OAuth 2.0, https://oauth.net/2/.OpenID Connect, http://openid.net/connect/.
Complementary	

Recommendations
Subjects that it is recommended to have taken before
Subjects that are recommended to be taken simultaneously
Subjects that continue the syllabus
Other comments

(*)The teaching guide is the document in which the URV publishes the information about all its courses. It is a public document and cannot be modified. Only in exceptional cases can it be revised by the competent agent or duly revised so that it is in line with current legislation.