Teaching Guide				
Identifying Data				2023/24
Subject (*)	Applications Security		Code	614530104
Study programme	Máster Universitario en Ciberseguridade			
Descriptors				
Cycle	Period	Year	Type	Credits
Official Master's Degree	1st four-month period	First	Obligatory	5
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.			

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
A24	HD-04 - Prevenir, identificar y corregir las principales vulnerabilidades que sufren las aplicaciones, así como incorporar mecanismos de autenticación, autorización y control de acceso a las aplicaciones
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
B20	K-04 - Distinguir las principales vulnerabilidades que sufren las aplicaciones, así como los principales mecanismos de autenticación, autorización y control de acceso, con énfasis especial en aplicaciones web y servicios web
C4	CT4 - Ability to ponder the importance of information security in the economic progress of society
C8	C-03 - Trabajar como analista de malware, para proteger aplicaciones, así como analizar su seguridad en cualquier área de aplicación
C19	C-14 - Proyectar, modelar, calcular y diseñar soluciones técnicas y de gestión de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación, con criterios éticos de responsabilidad y deontología profesional

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 AJ24	BJ2 BJ7 BJ20	CJ4 CJ8 CJ19
To know the techniques of authentication, authorization and access control in applications and services.	AJ2 AJ7 AJ13 AJ24	BJ2 BJ7 BJ20	CJ4 CJ8 CJ19

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 OAuth. 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 A24 B2 B7 B20 C4 C8 C19	24	24	48
ICT practicals	A2 A7 A13 A24 B2 B7 B20 C4 C8 C19	18	47	65
Multiple-choice questions	A2 A7 A13 A24 B2 B7 B20 C4 C8 C19	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. Tutorial timetables: - UDC teachers: https://www.udc.es/gl/centros_departamentos_servizos/centros/titorias/?codigo=614. - UVIGO teachers: https://moovi.uvigo.gal/user/profile.php?id=11662. 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 A24 B2 B7 B20 C4 C8 C19	Completion of the two projects is mandatory.	60
Multiple-choice questions	A2 A7 A13 A24 B2 B7 B20 C4 C8 C19	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: 0.40 * project1 + 0.20 * project2 + 0.40 * exam. Marks of projects and the test are saved from the first call to the second call (extraordinary at UVIGO).

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, https://oauth.net.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, https://oauth.net.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.