GENERAL INFORMATION

Data of the subject	
Subject name	App Security
Subject code	DTC-MCS-525
Mainprogram	
Involved programs	Máster en Ciberseguridad [Primer Curso]
Level	Master
Quarter	Semestral
Credits	4,5 ECTS
Type	Obligatoria
Department	Department of Telematics and Computer Sciencies
Coordinator	Rafael Palacios
Course overview	Nowadays, more than 80% of the attacks are mainly on web and mobile applications, so we must secure the applications. Therefore, we must understand the issues from the initial phases in which a programmer develops an algorithm to the final phase of deployment in production, when it is accessible to end users and hackers. The new development paradigms have led to the emergence of agile and organizational methodologies for the development of secure software. Therefore, we must know the Software Development Life Cycle (SDLC) and its methodologies, as well as the new approaches in DevSecOps. Finally, we will learn how to find (and mitigate) vulnerabilities in source code through automatic tools and manual review.

Teacher Information	
Teacher	
Name	Carlos Manchado Martín
Department	Department of Telematics and Computer Sciencies
EMail	cmanchado@icai.comillas.edu
Teacher	
Name	Miguel Enrique de Vega Martín
Department	Department of Telematics and Computer Sciencies
EMail	medevega@icai.comillas.edu

DESCRIPTION OF THE SUBJECT

Contextualization of the subject

Prerequisites

It is recommended to know how to program in at least one language, preferably Java or any Object Oriented language.

Course contents

Contents

Contents

Theory – SDLC y DevSecOps

1. Introduction to Application Security and SSDLC
2. Secure Development Framework - OWASP SAMM Model and MS DSL for Agile
3. Secure Development Framework - Standard Model I
4. Secure Development Framework - Standard Model II
5. DevSecOps and Container Security
6. Methodology and Software Life Cycle
7. Case Studies

Practice - Code and binary review

1. AppSec Introduction.
2. Overview and classic controls.
3. ACIDA model.
    - Authentication.
    - Authorization.
    - Confidentiality.
    - Integrity.
    - Availability.
    - Auditability.
4. Introduction to Secure Development.
5. Session management.
6. Data Validation.
7. Other general secure development controls.
8. Types of application audits.
    - Static Application Security Testing (SAST)
    - Dynamic Application Security Testing (DAST)
    - SAST vs DAST
9. Initiate an audit.
10. Tools for code review.
11. Methodologies.
12. Code review (SAST).
13. Dependency Review (SCA).
14. Final audit report.
15. Introduction to reverse engineering.

16. Reverse Engineering in Java.
17. Reverse engineering in mobile applications.
    - Android.
    - iOS.
18. Reverse engineering in libraries.
19. Reverse engineering in binaries.

EVALUATION AND CRITERIA

Grading

The course is composed of 4.5 credits, being the distribution:

- Theory - SDLC and DevSecOps: 1.5 credits.
- Practice - Code and binary review: 3.0 credits.

The evaluation includes an exam and a final work:

- Theory - SDLC and DevSecOps:
    - Exam: 35% (final grade of the course).
- Practice - Review of code and binaries:
    - Examination: 35% (final grade of the course)
    - Final work: 30% (final grade of the course).

BIBLIOGRAPHY AND RESOURCES

Basic References

The sources used during the course are Safety standards such as:

- OWASP

- NIST

- MITRE