Universidad Zaragoza

Academic Year/course: 2023/24

62240 - Exploiting Software Vulnerabilities

Syllabus Information

Academic year: 2023/24
Subject: 62240 - Exploiting Software Vulnerabilities
Faculty / School: 110 - Escuela de Ingeniería y Arquitectura
Degree: 534 - Master's Degree in Informatics Engineering
ECTS: 3.0
Year:
Semester: First semester
Subject type: Optional
Module:

1. General information

By taking this course, students will be able to analyze code and software systems to identify and solve the most common vulnerabilities and security problems. Thus, they will be able to apply various techniques to analyze security and compromise vulnerable software systems, reliably demonstrating the existing problems and proposing appropriate improvement solutions.

These approaches and objectives are aligned with the following Sustainable Development Goals (SDGs) of the United Nations 2030 Agenda (https://www.un.org/sustainabledevelopment), in such a way that the acquisition of the learning results of the course provides training and competence to contribute to a certain extent to its achievement. Specifically, they are aligned with the following objectives: Goal 9.1 and Goal 11.2.

2. Learning results

Each student must be able to:

- RA1: Recognize the most common vulnerabilities in software systems.
- RA2: Evaluate the security of a software system.
- RA3: Mastering different software systems analysis techniques.
- RA4: Create proofs of concept that allow compromising the security of vulnerable software systems.

3. Syllabus

- Introduction: vulnerability management, types of vulnerabilities, tools and analysis lab
- Program binary analysis: static analysis, dynamic analysis. Ethical concerns
- Software vulnerabilities and exploitation techniques: memory errors (in heap, in stack), integers, format strings, concurrency issues
- Software defenses
- Advanced exploitation techniques: ROP attacks, custom shellcode design

4. Academic activities

The course (75 hours) includes the following learning tasks:

- 26 hours, approximately, of classroom activities: lectures, laboratory sessions, and problem-solving tasks.
- 30 hours, approximately, of assignments and research projects.
- 5 hours, approximately, of tutorials.
- 10 hours, approximately, of autonomous work and study.
- 4 hours, approximately, of the exam and defense of the course project.

5. Assessment system

The student must demonstrate that they have achieved the expected learning outcomes through the following assessment activities:

- Practical work [70%]. The presentation and defense of practical programming work will be valued with a practical qualification that will weigh 70% of the final grade for the subject. With this test the learning results RA1, RA2, RA4 will be evaluated.
- Problem solving [30%]. A final evaluation test will be carried out, consisting of a presentation of group work, which will serve to demonstrate that the learning outcomes required in the subject have been achieved. Problems of a similar nature to those raised in class (code analysis and proof of concept) will be solved. The grade obtained in this test will weigh 30% of the final grade for the subject. With this test the learning outcomes RA1, RA2, RA3, and RA4 will be

evaluated.

The student who does not opt for the evaluation procedure described above, or does not pass the tests during the teaching period, or wants to improve their grade, will have the right to take a global test that will be scheduled within the exam period corresponding to the first or second call.