Universitat Autònoma de Barcelona

2021/2022

Software Security and Vulnerability

Code: 104376
ECTS Credits: 6

Degree	Type	Year	Semester
2503758 Data Engineering	OT	4	0

The proposed teaching and assessment methodology that appear in the guide may be subject to changes as a result of the restrictions to face-to-face class attendance imposed by the health authorities.

Contact

Name: Elisa Ruth Heymann Pignolo
Email: Elisa.Heymann@uab.cat

Use of Languages

Principal working language: spanish (spa)
Some groups entirely in English: No
Some groups entirely in Catalan: No
Some groups entirely in Spanish: Yes

Prerequisites

Familiar with a programing language such as Java, Python o C/C++.

Objectives and Contextualisation

Teaches the security considerations that occur during all steps of the software development life cycle: methodologies for designing secure software, programming using secure programming techniques, in-depth vulnerability assessment methodologies, static and dynamic analysis tools for evaluating software security, and system defenses reducing security threats.

Competences

- Conceive, design and implement efficient and secure data storage systems.
- Prevent and solve problems, adapt to unforeseen situations and take decisions.
- Students must be capable of collecting and interpreting relevant data (usually within their area of study) in order to make statements that reflect social, scientific or ethical relevant issues.
- Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.
- Work cooperatively in complex and uncertain environments and with limited resources in a multidisciplinary context, assuming and respecting the role of the different members of the group.

Learning Outcomes

1. Prevent and solve problems, adapt to unforeseen situations and take decisions.
2. Students must be capable of collecting and interpreting relevant data (usually within their area of study) in order to make statements that reflect social, scientific or ethical relevant issues.
3. Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.

4. Study the adaptations made to data analysis and consultation algorithms in order for these to maintain the privacy of the entry data, of the models learnt, or of the outputs of the models used in the field of business intelligence.
5. Work cooperatively in complex and uncertain environments and with limited resources in a multidisciplinary context, assuming and respecting the role of the different members of the group.

Content

1. Introduction and basic terminology.

2. Thinking like an attacker.

3. Secure programing:

3.1. Buffer overflow.

3.2. Numeric Errors.

3.3. Serialization.

3.4. Exeptions.

3.5. Injection attacks.

3.5.1. SQL Injection.

3.5.2. Command injection.

3.5.3. XML Injection.

3.5.4. Code Injection.

3.6. Directory traversal.

3.7. Web attacks.

3.7.1. Cross Site Scripting (XSS)

3.7.2. Cross Site Request Forgery (CSRF).

3.7.3. Session management.

3.7.4. Redirections.

3.8. Security for mobile devices.

4. Secure design. Thread modeling.

5. Vulnerability detection. FPVA methodology.

6. Tools for finding vulnerabilities.

7. Fuzz testing.

Methodology

There are 4 hours of teaching per week, divided into 2 sessions of 2 hours. During each session a theoretical topic will be exposed and practical exercises related to the exposed topic will be solved. This requires students to have their own laptop.

The content of each class will be detailed in the program that will be available on virtual campus before the first day of class.

Annotation: Within the schedule set by the centre or degree programme, 15 minutes of one class will be reserved for students to evaluate their lecturers and their courses or modules through questionnaires.

Activities

Title	Hours	ECTS	Learning Outcomes
Type: Directed			
Autonomous activities	100	4	4, 1, 3, 2, 5
Lectures including lab exercises	44	1.76	4, 1, 3, 2, 5

Assessment

There will be 2 or 3 examps duringthe term. The weight of these exams is 60%.

Each topic covered in class will have a related lab execise. Students will have to deliver a handout about their solutions. The weight of these exercises is 40%.

Assessment Activities

Title	Weighting	Hours	ECTS	Learning Outcomes
2 or 3 exams	60%	3	0.12	4, 1, 3, 2, 5
Lab exercises	40%	3	0.12	4, 1, 3, 2, 5

Bibliography

Introduction to Software Security by Loren Kohnfelder, Elisa Heymann and Barton Miller. Available from: http://research.cs.wisc.edu/mist/SoftwareSecurityCourse/

Software

Students will receive a VirualBox image that will contain all the necessary software to perform most exercises. This software includes programming languages and multiple tools.

Students will need to download and install Android studio to program mobile devices.

They will also have to download MS Thread Modeling Tool.