Course guide
330733 - DS - Database Security

Last modified: 10/07/2025

Unit in charge: Manresa School of Engineering
Teaching unit: 750 - EMIT - Department of Mining, Industrial and ICT Engineering.

Degree: MASTER'S DEGREE IN MACHINE LEARNING AND CYBERSECURITY FOR INTERNET-CONNECTED SYSTEMS (Syllabus 2024). (Optional subject).

Academic year: 2025 **ECTS Credits:** 3.0 **Languages:** English

LECTURER

Coordinating lecturer: Adarsh Kumar

Others:

TEACHING METHODOLOGY

AF1. Attendance and participation in master class. Presentation in class of new content and description of the study materials by the teacher and questions by the students to the teacher in relation to the content that he is explaining or presenting in the master class.
AF2. Attendance and participation in participatory class. Presentation of problems, challenges or case studies that students solve individually or in groups, with the teacher's assistance.
AF3. Carrying out laboratory practice. Completion in the laboratory and under the supervision of the teacher of tasks and experiments defined in the practice script, related to the implementation of the contents of the subject. It normally requires the preparation of a prior study and the preparation of a subsequent report. Possible field trips are considered within this typology.
AF4. Completion of tasks related to project-based learning. Students meet and manage the development of a complex project, organizing and distributing the necessary tasks and resources.
AF5. Presentation and defense of works. Students present to the rest of the class and the teacher how they have carried out the proposed tasks, be it solving problems, carrying out practices or developing projects.
AF6. Autonomous study carried out by the student outside of class hours. The student, autonomously, studies the content taught by the teacher, through notes and other materials provided by the teacher or obtained by the student himself.
AF7. Autonomous work carried out by the student outside of class hours. Tasks carried out autonomously, either individually or in a team, consisting of problem solving, exercises or the development of practices.
AF8. Attendance at tutoring session. Meeting of the student with the teacher or tutor to resolve specific doubts about content and tasks and assess the student's own progress.

LEARNING OBJECTIVES OF THE SUBJECT

- M.6.1 (K) Identify open source tools and other resources to monitor network security in a production environment.
- M.6.3 (K) Recognize the architecture of a system and the interfaces between components to keep the system secure.
- M.6.4 (S) Implement advanced security solutions using cryptographic schemes and standards.
- M.6.6 (S) Apply best practices for the design and implementation of secure databases and the development of robust, non-vulnerable applications with tools that facilitate integration, maintenance and continuous testing.
- M.6.7 (S) Implement contingency mechanisms that minimize the impact of a security breach and allow rapid recovery in industrial control systems.

CONTENTS

Unit 1. Introduction to Database Security

Description:
- CIA principles applied to databases
- Common threats in relational database systems (SQLi, privilege escalation, data leakage)
- Security regulations: GDPR, HIPAA, ISO/IEC 27001

Related activities:
All the relevant ones.

Full-or-part-time: 9h
Theory classes: 1h 30m
Laboratory classes: 1h 30m
Self study : 6h

Unit 2. User Management and Access Control

Description:
- User and password policies
- Role-based access control (RBAC)
- Privileges and auditing: GRANT, REVOKE, role-based audit trails

Related activities:
All the relevant ones.

Full-or-part-time: 9h
Theory classes: 1h 30m
Laboratory classes: 1h 30m
Self study : 6h

Unit 3. Secure Database Configuration

Description:
- Security parameters in database configuration files (e.g., my.cnf, postgresql.conf)
- Disabling unused features and ports
- Logging and monitoring

Related activities:
All the relevant ones.

Full-or-part-time: 9h
Theory classes: 1h 30m
Laboratory classes: 1h 30m
Self study : 6h

Unit 4. Injection Attacks and Input Validation

Description:
- Types of injection: SQL, XML, code injection
- Use of prepared statements and ORMs
- Input validation and escaping strategies

Related activities:
All the relevant ones.

Full-or-part-time: 9h
Theory classes: 1h 30m
Laboratory classes: 1h 30m
Self study : 6h

Unit 5. Backup and Disaster Recovery

Description:
- Full, incremental, and differential backups
- Automated backup strategies
- Secure storage and restoration processes
- Data manipulation, privilege escalation, or unauthorized transactions

Related activities:
All the relevant ones.

Full-or-part-time: 9h
Theory classes: 1h 30m
Laboratory classes: 1h 30m
Self study : 6h

Unit 6. Network-Level Database Security

Description:
- Firewall, IP restriction and access policies
- Connection encryption with SSL/TLS
- VPN and SSH tunneling for remote access

Related activities:
All the relevant ones.

Full-or-part-time: 10h
Theory classes: 1h 30m
Laboratory classes: 1h 30m
Self study : 7h

Unit 7. Modern Open Source Databases and Security Features

Description:
- Security features in PostgreSQL, MariaDB, MongoDB
- Authentication methods: SCRAM, LDAP, X.509
- Replication security and cluster hardening

Related activities:
All the relevant ones.

Full-or-part-time: 10h
Theory classes: 1h 30m
Laboratory classes: 1h 30m
Self study : 7h

Unit 8. Advanced Threats in Database Environments

Description:
- Insider threats and privilege abuse
- Data exfiltration and covert channels
- Anomaly detection, honeypots, and deception in databases
- Stored Cross-Site Scripting (XSS), Blind SQL Injection, Command Injection via Database Functions, Database Backdoor Installation

Related activities:
All the relevant ones.

Full-or-part-time: 10h
Theory classes: 1h 30m
Laboratory classes: 1h 30m
Self study : 7h

ACTIVITIES

Lectures

Description:
Face-to-face teacher-led learning sessions specifically focused on understanding the subject content. Lectures are provided by either the professors assigned to this course or guest lecturer from the industry.

Material:
Slide decks and other notes prepared and distributed by the lecturer.

Delivery:
Participation and technical discussions will determine the overall grade variable PAR.

Full-or-part-time: 12h
Theory classes: 12h

Independent Study

Description:
Independent study consists of studying to understand and solidify knowledge, vocabulary and techniques either alone or in a group. It includes reading material from bibliography or through independent search.

Material:
The support materials are:
- Slide decks and other notes prepared and distributed by the lecturer
- Main references of the subject.

Full-or-part-time: 43h
Self study: 43h

Laboratory work

Description:
Students practices implementing secure database systems. This includes hands-on learning with face-to-face tutorials, as well as practical assignments. This may mean completing practicals during independent learning time.

The practical sessions are as follows:
Practice 1 – Secure Installation and Configuration
Practice 2 – Role and Permission Management
Practice 3 – Log Monitoring and Event Analysis
Practice 4 – Injection Attack Simulation and Prevention
Practice 5 – Secure Backups and Restoration
Practice 6 – Network Security for Database Access
Practice 7 – Security Assessment and Hardening

Material:
Instruction sheets provided by the lecturer and use cases provided by guest lecturers.

Delivery:
The requirements gathering exercises and reports to be produced by the students counts as overall grade variable LAB. A practical exam or project counts as PR.

Full-or-part-time: 12h
Laboratory classes: 12h

Exam

Description:
There will be a final exam consisting of a set of exercises to be solved on paper without any support material, in a short amount of time and by working alone.

Delivery:
The individual exam solutions are delivered and evaluated. The exam grade corresponds to the course grade variable FIN.

Full-or-part-time: 8h
Self study: 8h

GRADING SYSTEM

The final grade is calculated with the following weights:

Overall grade = 0.4 * FIN + 0.1 * PAR + 0.30 * LAB + 0.20 * PR

BIBLIOGRAPHY

Basic:
- Kim, David ; Solomon, Michael G. Fundamentals of information systems security [on line]. Fifth edition. Jones & Bartlett Learning, 2021 [Consultation: 13/10/2025]. Available on: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=32293539. ISBN 1-284-31070-1.
- OWASP Top 10 – Web Application Security Risks [on line]. OWASP Foundation, 2023 [Consultation: 07/10/2025]. Available on: https://owasp.org/Top10/.
- PostgreSQL Documentation [on line]. PostgreSQL Global Development Group, 2024 [Consultation: 07/10/2025]. Available on: https://www.postgresql.org/docs/.
- MariaDB Server Documentation [on line]. MariaDB Foundation, 2024 [Consultation: 07/10/2025]. Available on: https://mariadb.org/documentation/.
- MongoDB Security Manual [on line]. MongoDB Inc, 2024 [Consultation: 07/10/2025]. Available on: https://www.mongodb.com/.
- SP 800-53 Rev. 5: Security and Privacy Controls [on line]. NIST, 2024 [Consultation: 07/10/2025]. Available on: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
- Wazuh Documentation for log integration with databases [on line]. Wazuh., [Consultation: 07/10/2025]. Available on: https://documentation.wazuh.com/.
- CIS Benchmarks for MySQL, PostgreSQL, and MongoDB [on line]. Center for internet security, [Consultation: 07/10/2025]. Available on: https://www.cisecurity.org/cis-benchmarks.