Module Specification

Introduction to Databases

Version: 2025-26, v2.0, Approved

Contents

Part 1: Information

Module title: Introduction to Databases

Module code: UFCFTK-30-1

Level: Level 4

For implementation from: 2025-26

UWE credit rating: 30

ECTS credit rating: 15

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: This module will equip cyber security students to understand the design and role of database applications in the modern workplace. Students will develop theoretical knowledge and practical skills in the design and build of a web-based end-to-end relational database application. Having implemented this, students will go on to gain valuable experience in detecting security vulnerabilities, while also understanding alternative database techniques (e.g. NoSQL). The business and legal contexts of database applications will also be considered.

Features: Not applicable

Educational aims: The educational aims of the module are to have hands-on experience of designing and developing a modern web application. They will also have an opportunity to analyse database security issues. Both assessments are individual, but the practical sessions and online materials combine to develop a supportive and collaborative learning environment.

Outline syllabus: Database Design Process: from business requirements to entity relationship modelling, including E-R diagramming techniques. Database schemas. Normalisation to 3NF (Third Normal Form). Avoiding data redundancy and anomalies.

Structured Query Language (SQL): table creation, maintenance, queries, calculations, grouping, joining tables, subqueries, views. (Using a suitable Data Base Management System (DBMS) (for example MySQL Server). Factors affecting query performance.

Database security: Data integrity, avoiding update anomalies. Legal considerations (e.g. General Data Protection) and security by design. Corporate and social importance of securing personal data. Range of attacks/vulnerabilities on relational and NoSQL databases, including SQL injection.

Developing an end-to-end database application: Client-server model. How basic HTML, Cascading Styling Sheets (CSS) and JavaScript interact via a suitable server and programming language (e.g. Python Flask) to backend. Use of connectors e.g. Open Data Base Connectivity (ODBC).

Relational databases and newer alternatives. Overview of NoSQL database types and comparison of advantages and disadvantages over relational techniques.

Part 3: Teaching and learning methods

Teaching and learning methods: Scheduled learning:

The main material in the module will be introduced in lectures. This theoretical exposure to the material will then be supplemented by practical lab sessions using a relational database, like Mysql. Also, a programming language will be introduced working with a database. The students will also get experience working with a noSQL database.

Independent learning:

In addition, students will be expected to develop independent learning approaches through directed reading, study and self-paced quizzes and exercises to reinforce, critically appraise and reflect upon concepts and techniques presented in lectures.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Understand the principles of the design and development of databases through data modelling and data manipulation using appropriate contemporary tools.

MO2 Utilise web and application programming languages to build and interact with a database back-end, performing essential operations for data retrieval and manipulation.

MO3 Demonstrate knowledge of a range of vulnerabilities and countermeasures in the design and operation of databases.

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 228 hours

Face-to-face learning = 72 hours

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://uwe.rl.talis.com/modules/ufcftk-30-1.html

Part 4: Assessment

Assessment strategy: The assessment strategy will consist of two coursework tasks. Both tasks will be based on material covered in lectures and practicals, with guidance offered to the students during practicals.

At both first sit and resit, the assessment tasks are:

Task 1 (60%)

Document and demonstrate the design and build of a small end-to-end database application according to a client's specification. Develop a web-based front end and use a suitable connector to perform select, insert, delete and update queries.

Task 2 (40%)

The task requires an analysis of security vulnerabilities in a relational end-to-end database application and demonstrate an understanding of how contemporary techniques could influence the hosting, querying and security of the application.

Opportunities for formative feedback are built into module delivery through in-class practical sessions. Session materials will be a mix of in-house guides created by the module team and open-source materials. Guidance will be provided through self-directed learning, class activities, in-class discussions and by giving informal feedback on practical session activities.

Assessment tasks:

Portfolio (First Sit)
Description: Implementation, Testing and Evaluation of Database Application (with a Demo)
Weighting: 60 %
Final assessment: No
Group work: No

Learning outcomes tested: MO1, MO2

Written Assignment (First Sit)
Description: Database Design (1500 - 2000 words)
Weighting: 40 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO2, MO3

Portfolio (Resit)
Description: Implementation, Testing and Evaluation of Database Application (with a Demo)
Weighting: 60 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2

Written Assignment (Resit)
Description: Database Design (1500 - 2000 words)
Weighting: 40 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO2, MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Digital Forensics {Foundation} [Frenchay] BSc (Hons) 2024-25

Cyber Security and Digital Forensics {Foundation} [Frenchay] BSc (Hons) 2024-25

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2025-26

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2025-26