MODULE SPECIFICATION

Part 1: Information			
Module Title	Webapp Development		
Module Code	UFCFTM-15-1	Level	Level 4
For implementation from	2020-21		
UWE Credit Rating	15	ECTS Credit Rating	7.5
Faculty	Faculty of Environment & Technology	Field	Computer Science and Creative Technologies
Department	FET Dept of Computer Sci & Creative Tech		
Module type:	Standard		
Pre-requisites	None		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description

Educational Aims: See Learning Outcomes

Outline Syllabus: Plan, develop and test interactive WebApps using suitable client and server side scripting languages. These could include:
Client-side; e.g. HTML5, CSS3, JavaScript, jQuery
Server-side; e.g. PHP, ASP, Ruby/Rails
Frameworks; e.g. jQuery, AngularJS, React. Laravel, APIs; e.g. SOAP, REST, JSON

Use a suitable database engine e.g. SQL/NoSQL. Built a secure, performance-optimised database solution to power a WebApp

Develop professional user interfaces for at least one user level

Build and publish/deploy the completed project to a suitable enterprise webserver or hosting platform for general availability

Explain what penetration testing is and how it contributes to information assurance

Complete penetration testing on a platform and record findings (e.g. SQL/code injection, data sanitisation, LFI/RFI, XSS, DDoS, brute force attacks)

Teaching and Learning Methods: Introductory lectures are supported by seminars, case studies, visits and practical workshops. In addition this module will be supported by interactive forums and learning tools.

150 hours study time of which 36 hours will represent scheduled learning. Scheduled learning includes lectures, seminars, tutorials, demonstration, practical classes and workshops; external visits; supervised time in studio/workshop.

Independent learning includes hours engaged with essential reading, case study preparation, assignment preparation and completion. Apprentice study time will be organised each week with a series of both essential and further readings and preparation for practical workshops. It is suggested that preparation for lectures, practical workshops, session delivery and seminars will take 7 hours per week.

36 hours scheduled learning

114 hours research, independent study and preparation for assessment work

Scheduled learning will typically include lectures, seminars, supervision, external visits and an interactive forum.

All apprentices are expected to attend a series of tutorials.

Part 3: Assessment

This module is assessed by a combination of techniques: an examination and a practical portfolio.

Exam (includes the following):

Explain some of the common authentication and security considerations facing web application developers and hosts as per the prescribed syllabus content.
An analysis of the computing and security needs in a given case study
Describe common penetration testing processes and how they can be applied to WebApp testing and application development cycle

Practical Portfolio (includes the following):

Evidence of planning and design of a WebApp to support a business scenario
Implementation of a WebApp to support a business scenario Deploying and test a completed WebApp in a live/enterprise environment

Opportunities for formative assessment exist for the assessment strategy used. Verbal feedback is given and all apprentices will engage with personalised tutorials setting SMART targets as part of the programme design.

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Examination (Online) - Component A	✓	30 %	Online Multiple Choice Exam
Portfolio - Component B		70 %	Design, build, publish and test a business webapp to meet a defined requirement
Resit Components	**Final Assessment**	**Element weighting**	**Description**

Examination (Online) - Component A	✓	30 %	Online Multiple Choice Exam
Portfolio - Component B		70 %	Design, build, publish and test a business webapp to meet a defined requirement

Part 4: Teaching and Learning Methods

Learning Outcomes

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

Module Learning Outcomes	**Reference**
Explain common security risks present when building and publishing public facing web applications and best practice security and authentication (e.g. SQL injection protection, code injection/data validation, protection from brute force attacks, encryption and hashing techniques)	MO1
Explain penetration testing and how it contributes to information assurance using examples or scenarios	MO2
Plan, design, implement and test a WebApp to support a business scenario	MO3
Implement a secure WebApp back-end demonstrating best practice security and authentication (e.g. SQL injection protection, code injection/data validation, protection from brute force attacks)	MO4
Build, manage and deploy the completed project into an enterprise hosting environment	MO5
All data must be stored and retrieved from an appropriately structured SQL database	MO6

Contact Hours

Independent Study Hours:	
Independent study/self-guided study	114
Total Independent Study Hours:	114
Scheduled Learning and Teaching Hours:	
Face-to-face learning	36
Total Scheduled Learning and Teaching Hours:	36
Hours to be allocated	150
Allocated Hours	150

Reading List

The reading list for this module can be accessed via the following link:

https://uwe.rl.talis.com/index.html

Part 5: Contributes Towards
This module contributes towards the following programmes of study: