ZAPP H4201: Secure Application Development

Module Title:	Secure Application Development

Credits:	5

NFQ Level:	8

Module Delivered In	No Programmes

Teaching & Learning Strategies:	As well as traditional lectures learners will undertake various laboratory exercises. Learners will be expected to actively participate in class on the materials covered and work throughout each scheduled lab session to accomplish assigned tasks.

Module Aim:	To provide learners with a theoretical knowledge and practical skills of developing secure software applications, with particular emphases on web technologies.

Learning Outcomes	
On successful completion of this module the learner should be able to:	
LO1	Evaluate and discuss the most prevalent software application security issues.
LO2	Analyse application design for security weaknesses.
LO3	Perform security testing to identify and validate the existence of software vulnerabilities.
LO4	Formulate and deploy strategies to fix or mitigate against identified vulnerabilities.

Pre-requisite learning
Module Recommendations *This is prior learning (or a practical skill) that is recommended before enrolment in this module.*
No recommendations listed
Incompatible Modules *These are modules which have learning outcomes that are too similar to the learning outcomes of this module.*
No incompatible modules listed
Co-requisite Modules
No Co-requisite modules listed
Requirements *This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed.*
No requirements listed

ZAPP H4201: Secure Application Development

Module Content & Assessment

Indicative Content
Secure Software Development Secure software life cycle, secure application design, secure mobile application development, cryptographic Design & implementation.
Data Validation & Access Control Input validation and sanitisation, output encoding, authentication and password management, session management, access control.
Error Management and Information Disclosure Error handling and logging, environment configuration, minimising Information Disclosure
Resource Security Communication security, system configuration, database security, file access management, memory management.
System Penetration Testing & Code Analysis Vulnerabilities code analysis and mitigations as outlined by leading industry security bodies such as OWASP, ISC2 and SANS.

Assessment Breakdown	%
Continuous Assessment	10.00%
Project	30.00%
End of Module Formal Examination	60.00%

Continuous Assessment

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Examination	Assessment on semester 1 content.	1,2	5.00	Sem 1 End
Examination	Assessment on semester 2 content.	1,2	5.00	Sem 2 End

Project

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Project	To analyse the security flaws in a web application and perform code reviews and code fixes to mitigate identified vulnerabilities.	2,3,4	15.00	Sem 1 End
Project	Analyse the security flaws in a web application and perform code reviews and edits to mitigate identified vulnerabilities.	2,3,4	15.00	Sem 2 End

No Practical

End of Module Formal Examination

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Formal Exam	The terminal exam will be a 3 hour written test	1,2,3,4	60.00	End-of-Semester

SETU Carlow Campus reserves the right to alter the nature and timings of assessment

ZAPP H4201: Secure Application Development

Module Workload

Workload: Full Time		
Workload Type	*Frequency*	*Average Weekly Learner Workload*
Lecture	Every Week	1.00
Laboratory	Every Week	2.00
Independent Learning Time	Every Week	2.00
	Total Hours	5.00