H9SWD: Secure Web Development

Module Code:	H9SWD
Long Title	Secure Web Development APPROVED
Title	Secure Web Development
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	5
Module Coordinator:	Vanessa Ayala-Rivera
Module Author:	Andrea Del Campo Dugova
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	PhD/Master's degree in a computing or cognate discipline. May have industry experience also.

Learning Outcomes	
On successful completion of this module the learner will be able to:	
#	**Learning Outcome Description**
LO1	Critically evaluate common vulnerabilities of web applications with a view to identifying countermeasures to prevent such vulnerabilities from being exploited.
LO2	Critically assess the technological challenges associated with securing web applications from a programming perspective.
LO3	Evaluate and implement programming solutions for securing web applications.
LO4	Appraise the tools and techniques used to attack and test web applications to strengthen their security.
LO5	Critically assess methodologies and artifacts involved in the Secure Software Development Lifecycle to design and implement secure web applications.

Dependencies
Module Recommendations
No recommendations listed
Co-requisite Modules
No Co-requisite modules listed

Entry requirements	Programme entry requirements must be satisfied.

H9SWD: Secure Web Development

Module Content & Assessment

Indicative Content
Secure Software Engineering– Part 1 Introduction to Software Engineering; The Software Development Lifecycle (SDLC); Software Development Methodologies; Secure SDLC: Requirements (e.g., Security requirements).
Secure Software Engineering – Part 2 Secure SDLC (cont'd): Design (e.g., Security by Design principles, Threat modelling); Implementation (e.g., Static Analysis); Verification (e.g., Dynamic Analysis).
Introduction to Web Applications and Web Security Web Applications Architecture (client-side, server-side, storage, etc.); The HTTP protocol (requests, responses, headers); Data Encoding; Introduction to Web Security.
Web Browser Security How browsers work internally; Browser Architecture; Site Isolation and Sandboxing; Same Origin Policy and Cross-Origin Communication; Cookies' security model.
Web Application Vulnerabilities & Defences – Part 1 OWASP Top 10; Cross-site Scripting (XSS); Cross-site request forgery (CSRF)
Web Application Vulnerabilities & Defences – Part 2 SQL and noSQL Injection; Code/Command Injection
Web Application Vulnerabilities & Defences – Part 3 Identification and Authentication Failure: Authentication weaknesses, Password Attacks, NIST Password Guidelines, Multi-factor authentication; Defences.
Web Application Vulnerabilities & Defences – Part 4 Authorization Mechanisms; Session Management; Access Control Models; Session Hijacking, Session fixation; Clickjacking.
Security in Web Development Frameworks Inbuilt security features in web development frameworks (e.g., parameterized SQL Queries, secure session implementation, secure authentication, whitelisting on inputs, etc.)
Web Application Security Testing -Part 1 The Economics of Software Quality; Testing Tools and Processes; Security Testing Principles.
Web Application Security Testing -Part 2 Testing Practices (e.g., OWASP Web Security Testing Framework); Writing Test Cases for Software.
Web Application Security Testing – Part 3 Static application security testing (SAST) and Dynamic application security testing (DAST); Web Application Penetration Testing

Assessment Breakdown	%
Coursework	100.00%

Assessments

Full Time

Coursework

Assessment Type:	Formative Assessment	**% of total:**	Non-Marked
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4,5
Non-Marked:	Yes		

Assessment Description:
Formative assessment will be provided on the in-class individual or group activities. Feedback will be provided in written or oral format, or on-line through Moodle. In addition, in class discussions will be undertaken as part of the practical approach to learning.

Assessment Type:	Continuous Assessment	**% of total:**	40
Assessment Date:	n/a	**Outcome addressed:**	1,5
Non-Marked:	No		

Assessment Description:
Practical work will be conducted throughout the semester to assess the learner's evaluation skills in terms of secure software engineering and secure application development.

Assessment Type:	Project	**% of total:**	60
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4,5
Non-Marked:	No		

Assessment Description:
Learners are required to complete a web application development project where they incorporate practices and artifacts of secure software development lifecycle. Learners have to operationalize secure design principles and apply fixes to web security vulnerabilities. The web application will be insecure by default (either taking a project from a code repository or learners developing the application). Learners must compile an associated report and evaluate the security strength of the resulting application.

No End of Module Assessment

No Workplace Assessment

Reassessment Requirement

Coursework Only
This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Reassessment Description
The reassessment strategy for this module will consist of a project that will assess all learning outcomes.

H9SWD: Secure Web Development

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Independent Learning Time	Independent learning	77	Per Semester	6.42
Tutorial	Mentoring and small-group tutoring	24	Per Semester	2.00
			Total Weekly Contact Hours	4.00

Workload: Blended

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	12	Per Semester	1.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Directed Learning	Directed e-learning	24	Per Semester	2.00
Independent Learning	Independent learning	77	Per Semester	6.42
			Total Weekly Contact Hours	4.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	24	Per Semester	2.00
Independent Learning	Independent learning	77	Per Semester	6.42
			Total Weekly Contact Hours	4.00

Module Resources

Recommended Book Resources

Malcolm McDonald. (2020), Web Security for Developers, Real Threats, Practical Defense, No Starch Press, p.217, [ISBN: 1593279949].

Tanya Janca. (2020), Alice and Bob Learn Application Security, John Wiley & Sons, p.288, [ISBN: 1119687357].

Supplementary Book Resources

Dafydd Stuttard,Marcus Pinto. (2011), The Web Application Hacker's Handbook, John Wiley & Sons, p.912, [ISBN: 1118026470].

This module does not have any article/paper resources

Other Resources

[Website], OWASP,
https://www.owasp.org

[Website], Web for Pentester,
https://pentesterlab.com/exercises/web_f or_pentester

[Website], Web for Pentester 2,
https://pentesterlab.com/exercises/web_f or_pentester_II

[Website], Portswigger,
https://portswigger.net/web-security

[Website], Burp Suite,
https://portswigger.net/burp

[Website], OWASP ZAP,
https://owasp.org/www-project-zap/

Discussion Note:	