Module Descriptor

Title	Web Application Security Testing		
Session	2025/26	**Status**	Published
Code	COMP09109	**SCQF Level**	9
Credit Points	20	**ECTS (European Credit Transfer Scheme)**	10
School	**Computing, Engineering and Physical Sciences**		
Module Co-ordinator	Raman Singh		

Summary of Module

The aim of the module is to provide advanced web application testing and ethical hacking practices to provide students with an understanding of web application vulnerabilities including their causes and consequences as well as the methodologies for testing and how to protect applications.

Undertaking this module will develop a range of graduate attributes. Knowledge of the principles behind the techniques used to create secure web applications. Sourcing, reviewing and applying current best practices will develop critical thinking and analytical skills.

This module will work to develop a number of the key 'I am UWS' Graduate Attributes to make those who complete this module:

- Universal: Critical Thinker, Ethically minded, Research-minded
- Work Ready: Problem-Solver, Effective Communicator, Ambitious
- Successful: Autonomous, Resilient, Driven

Module Delivery Method	**On-Campus[1]**	**Hybrid[2]**	**Online[3]**	**Work -Based Learning[4]**
	☒	☐	☐	☐

Campuses for Module Delivery			
	☐ Ayr	☒ Lanarkshire	☐ Online / Distance Learning
	☐ Dumfries	☐ London	☐ Other (specify)
		☐ Paisley	

[1] Where contact hours are synchronous/ live and take place fully on campus. Campus-based learning is focused on providing an interactive learning experience supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus contact hours will be clearly articulated to students.

[2] The module includes a combination of synchronous/ live on-campus and online learning events. These will be supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus and online contact hours will be clearly articulated to students.

[3] Where all learning is solely delivered by web-based or internet-based technologies and the participants can engage in all learning activities through these means. All required contact hours will be clearly articulated to students.

[4] Learning activities where the main location for the learning experience is in the workplace. All required contact hours, whether online or on campus, will be clearly articulated to students

Terms for Module Delivery	Term 1	☐	Term 2	☒	Term 3	☐
Long-thin Delivery over more than one Term	Term 1 – Term 2	☐	Term 2 – Term 3	☐	Term 3 – Term 1	☐

Learning Outcomes	
L1	Demonstrate a critical understanding of the legal risks of web application testing;
L2	Demonstrate an understanding of secure web architecture and OWASP Top 10 security risks;
L3	Develop the skill to use a variety of tools to undertake rigorous security testing of the web applications;
L4	Develop skills to discover and exploit vulnerabilities in web applications;
L5	Recommend measures to improve the security of web applications;

Employability Skills and Personal Development Planning (PDP) Skills	
SCQF Headings	**During completion of this module, there will be an opportunity to achieve core skills in:**
Knowledge and Understanding (K and U)	**SCQF 9** A detailed understanding of the architecture of web applications, protection schemes for web applications, and cryptography for web applications.
Practice: Applied Knowledge and Understanding	**SCQF 9** The ability to use a variety of tools to discover and analyse the vulnerability of web applications.
Generic Cognitive skills	**SCQF 9** Systematic planning and undertaking of testing and hacking.
Communication, ICT and Numeracy Skills	**SCQF 9** Effective use of a variety of tools. Analytic skills in identifying the weaknesses and vulnerabilities of systems. Report writing and presentation skills.
Autonomy, Accountability and Working with Others	**SCQF 9** Teamwork skills.

Prerequisites	**Module Code** COMP07075 COMP08094	**Module Title** Security Fundamentals Ethical Hacking: Tools & Techniques
	Other	
Co-requisites	**Module Code**	**Module Title**

Learning and Teaching

In line with current learning and teaching principles, a 20-credit module includes 200 learning hours, normally including a minimum of 36 contact hours and maximum of 48 contact hours.

Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	**Student Learning Hours** (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture / Core Content Delivery	12
Tutorial / Synchronous Support Activity	12
Laboratory / Practical Demonstration / Workshop	24
Independent Study	152
Please select	
Please select	
TOTAL	200

Indicative Resources

The following materials form essential underpinning for the module content and ultimately for the learning outcomes:

Hoffman, A. (2024), Web Application Security: Exploitation and Countermeasures for Modern Web Applications. (2nd Edition), O'Reilly Media.

Harper, A., Eagle, C., Ness, J., Harris, S., Spasojevic, B., Regalado, D., Linn, R. and Sims, S. (2011) Grey Hat Hacking (4th Edition). McGraw-Hill.

Najera-Gutierrez, G. and Ansari, J.A. (2018) Web Penetration Testing with Kali Linux - Third Edition: Explore the methods and tools of ethical hacking with Kali Linux Paperback. (3rd Edition) Packt Publishing

Oracle Virtual Box along with guest additions and VirtualBox Extension Pack.

(N.B. Although reading lists should include current publications, students are advised (particularly for material marked with an asterisk*) to wait until the start of session for confirmation of the most up-to-date material)

Attendance and Engagement Requirements

In line with the Student Attendance and Engagement Procedure, Students are academically engaged if they are regularly attending and participating in timetabled on-campus and online teaching sessions, asynchronous online learning activities, course-related learning resources, and complete assessments and submit these on time.

For the purposes of this module, academic engagement equates to the following:

The School of Computing, Engineering and Physical Sciences considers attendance and engagement to mean a commitment to attending, and engaging in, timetabled sessions. You will scan your attendance via the scanners each time you are on-campus and you will login to the VLE several times per week. Where you are unable to attend a timetabled learning session due to illness or other circumstance, you should notify the Programme Leader that you cannot attend. Across the School an 80% attendance threshold is set. If you fall below

this, you will be referred to the Student Success Team to see how we can best support your studies.

Equality and Diversity
The University's Equality, Diversity and Human Rights Procedure can be accessed at the following link: UWS Equality, Diversity and Human Rights Code. Aligned with the University's commitment to equality and diversity, this module supports equality of opportunity for students from all backgrounds and learning needs. Using the VLE, material will be presented electronically in formats that allow flexible access and manipulation of content. This module complies with University regulations and guidance on inclusive learning and teaching practice. This module has lab-based teaching and as such you are advised to speak to the Module Co-ordinator to ensure that specialist assistive equipment, support provision and adjustment to assessment practice can be put in place, in accordance with the University's policies and regulations.
(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)

Supplemental Information

Divisional Programme Board	**Computing**
Overall Assessment Results	☐ **Pass / Fail** ☒ **Graded**
Module Eligible for Compensation	☒ **Yes** ☐ **No** **If this module is eligible for compensation, there may be cases where compensation is not permitted due to programme accreditation requirements. Please check the associated programme specification for details.**
School Assessment Board	Business & Applied Computing
Moderator	Althaff Mohideen
External Examiner	M Davis
Accreditation Details	
Module Appears in CPD catalogue	☒ **Yes** ☐ **No**
Changes / Version Number	1.07

Assessment (also refer to Assessment Outcomes Grids below)
Assessment 1
Practical Coursework (60%)
Assessment 2
Group Project (40%)
Assessment 3
(N.B. (i) Assessment Outcomes Grids for the module (one for each component) can be found below which clearly demonstrate how the learning outcomes of the module will be assessed. (ii) An indicative schedule listing approximate times within the academic calendar when assessment is likely to feature will be provided within the Student Module Handbook.)

Component 1							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Report of practical/field/ clinical work	☒	☒	☒	☐	☐		0

Component 2							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Dissertation/Project report/Thesis	☐	☐	☐	☒	☒		8

Component 3							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
	☐	☐	☐	☐	☐		
Combined total for all components						100%	8 hours

Change Control

What	When	Who
Attendance and Engagement and Equality and Diversity Statements	20/01/25	R Moffat
Guidance Note 23-24 provided & general Housekeeping to text across sections.	12/12/23	D Taylor
Updated Student Attendance and Engagement Procedure & UWS Equality, Diversity and Human Rights Code	19/10/23	C Winter
Updated contact hours	14/09/21	H McLean