This Version is No Longer Current
The latest version of this module is available here

MODULE DESCRIPTOR

Module Title

Web Security

Reference	CM3105	Version	3
Created	February 2019	SCQF Level	SCQF 9
Approved	July 2016	SCQF Points	15
Amended	February 2019	ECTS Points	7.5

Aims of Module

To provide students with an understanding of the main security threats to web based systems. To develop the students' skills in identifying weaknesses in web based systems and how to prevent or harden the systems against attack.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Identify and analyse web systems for possible security weaknesses.
2	Understand and explain how web system weaknesses can be exploited.
3	Critically appraise security techniques for the design of web based systems.
4	Implement security features to harden web based systems against attack.
5	Exploit known vulnerabilities to test the security of web based systems.

Indicative Module Content

Key concepts of identifying, exploiting and defending against web application or web system attacks. This will include aspects, which are the responsibility of the developer or system administrator such as server configuration, authentication mechanisms and application language configuration. The module will demonstrate a number of exploits and attacks that can be performed on web systems and methods to protect against them, including defacement, shell scripting, privilege escalation, cache poisoning, XPATH and XQUERY languages and injection, Cross-site request forging and application coding errors like SQL injection and cross-site scripting. The module will also look at vulnerabilities in the execution environments including web and mobile browser vulnerabilities and exploits. Standards and Best Practice Guides: ISO 27001, ISO 27014, ISO 27034.

Module Ref:	CM3105 v3

Module Delivery

Key concepts on design and development practices are introduced through the 1 hour lectures. The main emphasis of the course will be focused on the lab sessions where the students will be introduced to practical demonstrations of the exploits and defences being studied. The module will give the students access to custom configured web systems and applications with known vulnerabilities. Although these systems will be hosted in safe, sandboxed environments they will provide the students with a realistic platform on which to carry out simulated attack and defence practices. The final week of the module will pit the students against each other in a capture the flag exercise where teams will take turns to attack and defend a provided system.

Indicative Student Workload	Full Time	Part Time
Contact Hours	36	N/A
Non-Contact Hours	114	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	50%	Outcomes Assessed:	2, 3
Description:	Exam.				

Component 2

Type:	Practical Exam	Weighting:	50%	Outcomes Assessed:	1, 4, 5
Description:	Practical assessment.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 50% weighting of C1 and 50% weighting of C2. An overall minimum grade D is required to pass the module.

		Coursework:						
		A	**B**	**C**	**D**	**E**	**F**	**NS**
Examination:	**A**	A	A	B	B	C	E	
	B	A	B	B	C	C	E	
	C	B	B	C	C	D	E	
	D	B	C	C	D	D	E	
	E	C	C	D	D	E	E	
	F	E	E	E	E	E	F	
	NS	Non-submission of work by published deadline or non-attendance for examination						

Module Ref:	CM3105 v3

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1	SPASOJEVIC, B., 2015. Gray Hat Hacking The Ethical Hacker's Handbook. 4th ed.
2	SHEMA, M., 2012. Hacking web apps: detecting and preventing web application security problems. Syngress.
3	LONG, J., 2016. Google Hacking for Penetration Testers. Elsevier.
4	Computer Security Student - Web hacking tutorials https://computersecuritystudent.com [Accessed: July 2016].