

## MODULE DESCRIPTOR

### Module Title

Web & Mobile Security

Reference	CM3145	Version	1
Created	November 2023	SCQF Level	SCQF 9
Approved	April 2024	SCQF Points	15
Amended		ECTS Points	7.5

### Aims of Module

This module aims to empower students to identify and address security vulnerabilities in web and mobile systems, fostering proficiency in modern security strategies.

### Learning Outcomes for Module

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

- 1 Demonstrate skills in systematically identifying and analysing potential security weaknesses in web and mobile-based systems.
- 2 Demonstrate advanced proficiency in deploying strategies to exploit and defend against security weaknesses in modern web and mobile ecosystems.
- 3 Assess the effectiveness of implemented security methods to ensure a resilient defence posture for web and mobile-based systems.
- 4 Demonstrate proficiency in implementing industry standards and guidelines to mitigate security risks on web and mobile systems.

### Indicative Module Content

Core principles and methodologies: Webification, Application stores, Sandboxing, Permission based access control, Web Public Key Infrastructure (Web PKI) and HTTPS, Cookies, Web and mobile device authentication such as biometrics, graphical passwords, unlock patterns; Client-side vulnerabilities and mitigations: Phishing, Clickjacking, Client-side storage, Physical attacks; Server-side vulnerabilities and mitigations: Input sanitization, SQL-injection, Command injection, User-uploaded files, Local file inclusion, Cross-site scripting (XSS), Cross-site request forgery (CSRF); Server-side misconfiguration & vulnerable components: HeartBleed, Firewalls, Load balancers, Databases; Standards and Best Practice Guides.

### Module Delivery

Lectures introduce and illustrate key concepts, while practical skills are honed through a series of laboratory exercises.

**Indicative Student Workload**

	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	120	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
<i>Actual Placement hours for professional, statutory or regulatory body</i>		

**ASSESSMENT PLAN**

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

**Component 1**

Type: Coursework Weighting: 100% Outcomes Assessed: 1, 2, 3, 4

Description: Short term release and submit coursework covering all learning outcomes.

**MODULE PERFORMANCE DESCRIPTOR****Explanatory Text**

The calculation of the overall grade for this module is based on 100% weighting of Component 1. An overall minimum grade of D is required to pass this module.

Module Grade	Minimum Requirements to achieve Module Grade:
<b>A</b>	The student needs to achieve an A in Component 1
<b>B</b>	The student needs to achieve a B in Component 1
<b>C</b>	The student needs to achieve a C in Component 1
<b>D</b>	The student needs to achieve a D in Component 1
<b>E</b>	The student needs to achieve an E in Component 1
<b>F</b>	The student needs to achieve an F in Component 1
<b>NS</b>	Non-submission of work by published deadline or non-attendance for examination

**Module Requirements**

Prerequisites for Module	CM1131: Cybersecurity Fundamentals or equivalent prior learning
Corequisites for module	None.
Precluded Modules	None.

**INDICATIVE BIBLIOGRAPHY**

- 1 Hoffman, A. (2020). Web Application security: exploitation and countermeasures for modern web applications. O'Reilly Media.
- 2 Yaworski, P. (2019). Real-world bug hunting: a field guide to web hacking. No Starch Press.
- 3 Baker, M. (2022). Secure Web Application Development: A Hands-On Guide with Python and Django. Springer.
- 4 OWASP, ?OWASP cheat sheet series,? 2019. [Online]. Available: [https://www.owasp.org/index.php/OWASP\\_Cheat\\_Sheet\\_Series](https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series)
- 5 Au, M. H., Choo, R., & Lu, R. (2021). Mobile Security and Privacy: Advances, Challenges, and Future Research Directions. CRC Press.
- 6 Hoffman, A. (2020). ?Web Application security: exploitation and countermeasures for modern web applications. O'Reilly Media.