UNSW Course Outline

COMP6443 Web Application Security and Testing - 2024

Published on the 13 Feb 2024

General Course Information

Course Code : COMP6443
Year : 2024
Term : Term 1
Teaching Period : T1
Is a multi-term course? : No
Faculty : Faculty of Engineering
Academic Unit : School of Computer Science and Engineering
Delivery Mode : Multimodal
Delivery Format : Standard
Delivery Location : Kensington
Campus : Sydney
Study Level : Postgraduate, Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

Web applications are currently the predominant source of software vulnerabilities exploited in in online attacks. There is a growing need and growing demand for web programmers to be security aware.

This course covers the main types of web application vulnerabilities and current best practice professional coding and testing practices to be able to successfully develop secure web applications.

The course covers OWASP vulnerabilities cross site scripting browser security model and weaknesses Injection attacks DNS Man in the middle Data leakage Spoofing UI and Social vulnerabilities Assurance and Testing Standards. Course coverage will be constantly updated over time to reflect emerging vulnerabilities and practices.

A programming background is not required but it will be helpful in some of the more applied topics. Students need a keen devious and analytical mind. To get the most from this course students will need to engage in independent study and research and be able to act as independent self directed learners.

Course Aims

This course aims to

- extend students' understanding of security engineering
- study vulnerabilities in web applications, and how to exploit/defend them

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Have a knowledge of general web application security literacy, including the principal elements of contemporary web application vulnerabilities (such as cross site scripting, code injection, session stealing).
CLO2 : Understanding how these vulnerabilities are used by attackers, their characterising features, weaknesses and countermeasures.
CLO3 : Have an understanding of issues and key principles of secure web application design and be able to apply these to assess and test web applications and web sites;
CLO4 : Be able to work with web dev teams to design and create secure web applications.

Course Learning Outcomes	Assessment Item
CLO1 : Have a knowledge of general web application security literacy, including the principal elements of contemporary web application vulnerabilities (such as cross site scripting, code injection, session stealing).	• Portfolio • Final Exam
CLO2 : Understanding how these vulnerabilities are used by attackers, their characterising features, weaknesses and countermeasures.	• Portfolio • Final Exam
CLO3 : Have an understanding of issues and key principles of secure web application design and be able to apply these to assess and test web applications and web sites;	• Portfolio • Final Exam
CLO4 : Be able to work with web dev teams to design and create secure web applications.	• Portfolio

Learning and Teaching Technologies

Moodle - Learning Management System | WebCMS3

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Portfolio	35%	Due Date: TBA
Final Exam	65%	Due Date: During Exam Period

Assessment Details

Portfolio

Assessment Overview

Individually submitted portfolio to demonstrate Security Stream Capabilities.

Assessed by tutors on basis of claims and evidence and clarify of communication.

Course Learning Outcomes

- CLO1 : Have a knowledge of general web application security literacy, including the principal elements of contemporary web application vulnerabilities (such as cross site scripting, code injection, session stealing).
- CLO2 : Understanding how these vulnerabilities are used by attackers, their characterising features, weaknesses and countermeasures.
- CLO3 : Have an understanding of issues and key principles of secure web application design and be able to apply these to assess and test web applications and web sites;
- CLO4 : Be able to work with web dev teams to design and create secure web applications.

Final Exam

Assessment Overview

A final exam will be held in the CSE laboratories, involving both practical work and theory questions.

Course Learning Outcomes

- CLO1 : Have a knowledge of general web application security literacy, including the principal elements of contemporary web application vulnerabilities (such as cross site scripting, code injection, session stealing).
- CLO2 : Understanding how these vulnerabilities are used by attackers, their characterising features, weaknesses and countermeasures.
- CLO3 : Have an understanding of issues and key principles of secure web application design and be able to apply these to assess and test web applications and web sites;

General Assessment Information

Grading Basis

Standard

Course Schedule

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

General Schedule Information

The course is broken down into several topics:

- Week 1: Reconnaissance
- Week 2: Authentication & Authorisation
- Week 3: Authentication & Authorisation
- Week 4: SQLi
- Week 5: Server-side attacks
- Week 7: XSS
- Week 8: Client-Side attacks
- Week 9: DevSecOps
- Week 10: Advanced topics and further studies

Course Resources

Recommended Resources

Although there are no official textbooks for this course you may find the following books interesting and/or helpful to read / refer to. Let us know if there aren't enough copies in the library and we'll ask them to get more. It's a new and growing field with lots of pretty average books to waste your time -so if you find any books or materials you find helpful, please do share them with the rest of the course.

Reference Books:

Stuttard, Dafydd, and Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. John Wiley & Sons, 2012

Zalewski, Michal. The Tangled Web: a Guide to Securing Modern Web Applications. No Starch Press, 2012

Course Evaluation and Development

Toward the end of the term you will be asked to give feedback about the course via UNSW's MyExperience survey. Your feedback is valuable and will be used, along with feedback from other stakeholders, to help improve the course. You can also contact your Course Convenor, lecturers or tutors any time you have suggestions or other feedback

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Administrator	Rahat Masood					No	No
Convenor	Kristian Mansfield					Yes	Yes

Other Useful Information

Academic Information

I. Special consideration and supplementary assessment

If you have experienced an illness or misadventure beyond your control that will interfere with your assessment performance, you are eligible to apply for Special Consideration prior to, or within 3 working days of, submitting an assessment or sitting an exam.

Please note that UNSW has a Fit to Sit rule, which means that if you sit an exam, you are declaring yourself fit enough to do so and cannot later apply for Special Consideration.

For details of applying for Special Consideration and conditions for the award of supplementary assessment, please see the information on UNSW's Special Consideration page.

II. Administrative matters and links

All students are expected to read and be familiar with UNSW guidelines and polices. In particular, students should be familiar with the following:

- Attendance
- UNSW Email Address
- Special Consideration
- Exams
- Approved Calculators
- Academic Honesty and Plagiarism
- Equitable Learning Services

III. Equity and diversity

Those students who have a disability that requires some adjustment in their teaching or learning environment are encouraged to discuss their study needs with the course convener prior to, or at the commencement of, their course, or with the Equity Officer (Disability) in the Equitable Learning Services. Issues to be discussed may include access to materials, signers or note-takers, the provision of services and additional exam and assessment arrangements. Early notification is essential to enable any necessary adjustments to be made.

IV. Professional Outcomes and Program Design

Students are able to review the relevant professional outcomes and program designs for their streams by going to the following link: https://www.unsw.edu.au/engineering/student-life/student-resources/program-design.

Note: This course outline sets out the description of classes at the date the Course Outline is published. The nature of classes may change during the Term after the Course Outline is published. Moodle or your primary learning management system (LMS) should be consulted for the up-to-date class descriptions. If there is any inconsistency in the description of activities between the University timetable and the Course Outline/Moodle/LMS, the description in the Course Outline/Moodle/LMS applies.

Academic Honesty and Plagarism

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW students have a responsibility to adhere to this principle of academic integrity. Plagiarism undermines academic integrity and is not tolerated at UNSW. *Plagiarism at UNSW is defined as using the words or ideas of others and passing them off as your own.*

Plagiarism is a type of intellectual theft. It can take many forms, from deliberate cheating to accidentally copying from a source without acknowledgement. UNSW has produced a website with a wealth of resources to support students to understand and avoid plagiarism, visit: student.unsw.edu.au/plagiarism. The Learning Centre assists students with understanding academic integrity and how not to plagiarise. They also hold workshops and can help students one-on-one.

You are also reminded that careful time management is an important part of study and one of the identified causes of plagiarism is poor time management. Students should allow sufficient time for research, drafting and the proper referencing of sources in preparing all assessment tasks.

Repeated plagiarism (even in first year), plagiarism after first year, or serious instances, may also be investigated under the Student Misconduct Procedures. The penalties under the procedures can include a reduction in marks, failing a course or for the most serious matters (like plagiarism in an honours thesis or contract cheating) even suspension from the university. The Student Misconduct Procedures are available here:

www.gs.unsw.edu.au/policy/documents/studentmisconductprocedures.pdf

Submission of Assessment Tasks

Work submitted late without an approved extension by the course coordinator or delegated authority is subject to a late penalty of five percent (5%) of the maximum mark possible for that assessment item, per calendar day.

The late penalty is applied per calendar day (including weekends and public holidays) that the assessment is overdue. There is no pro-rata of the late penalty for submissions made part way through a day. This is for all assessments where a penalty applies.

Work submitted after five days (120 hours) will not be accepted and a mark of zero will be awarded for that assessment item.

For some assessment items, a late penalty may not be appropriate. These will be clearly indicated in the course outline, and such assessments will receive a mark of zero if not completed by the specified date. Examples include:

- Weekly online tests or laboratory work worth a small proportion of the subject mark;
- Exams, peer feedback and team evaluation surveys;
- Online quizzes where answers are released to students on completion;
- Professional assessment tasks, where the intention is to create an authentic assessment that has an absolute submission date; and,
- Pass/Fail assessment tasks.

Faculty-specific Information

Engineering Student Support Services – The Nucleus - enrolment, progression checks, clash requests, course issues or program-related queries

Engineering Industrial Training – Industrial training questions

UNSW Study Abroad – study abroad student enquiries (for inbound students)

UNSW Exchange – student exchange enquiries (for inbound students)

UNSW Future Students – potential student enquiries e.g. admissions, fees, programs, credit transfer

Phone

(+61 2) 9385 8500 – Nucleus Student Hub

(+61 2) 9385 7661 – Engineering Industrial Training

(+61 2) 9385 3179 – UNSW Study Abroad and UNSW Exchange (for inbound students)

School Contact Information

CSE Help! - on the Ground Floor of K17

- For assistance with coursework assessments.

The Nucleus Student Hub - https://nucleus.unsw.edu.au/en/contact-us

- Course enrolment queries.

Grievance Officer - grievance-officer@cse.unsw.edu.au

- If the course convenor gives an inadequate response to a query or when the course convenor does not respond to a query about assessment.

Student Reps - stureps@cse.unsw.edu.au

- If some aspect of a course needs urgent improvement. (e.g. Nobody responding to forum queries, cannot understand the lecturer)