Web Application Security & Testing - COMP6443

Extended Web Application Security & Testing - COMP6843

Course Outline 2022T2

These two courses run in an overlapping mode. Both share a set of common activities and assessments; however, 6843 students have additional extension activities and assessments related to penetration testing and professional security engineering in lieu of some of the core activities undertaken by 6443 students. The information below applies to both courses except where otherwise indicated.

Course Website

This course is hosted on Openlearning and that's where we'll all share information and communicate. In order to correctly link your Openlearning account to your zID the first time you access the Openlearning site must be via the link in Moodle.

1. Find the *Web Application Security & Testing* course page on Moodle; then
2. Click on the link to Openlearning.

Course Staff

Course Convenor: Rahat Masood

Lecturers:

- Norman Yue
- Abhijeth Dugginapeddi
- David Jorm
- Varun Chandramohan
- Marina Levi
- Yunsar Jillani

Technical Course Admin: Kristian Mansfield

How to contact us

- Speak/message with the lecturers at and after face-to-face lectures
- Speak with your tutor at/after zoom/face-to-face tutorials
- Chat with us and your classmates on the course website (OpenLearning)
- Confidential questions about course: cs6443@cse.unsw.edu.au
- Enquiries about Security Engineering major: SECedu@unsw.edu.au

Summary of the course

Web applications are currently the predominant source of software vulnerabilities exploited in online attacks worldwide. Most of these attacks exploit simple and easily remedied classes of security vulnerabilities. There is a clear and vastly unmet need for all web programmers to be security literate. There is also a substantial worldwide shortage of security professionals capable of assessing the security of Web Applications.

These related courses cover the main types of web application vulnerabilities and introduce current professional best practices in Web design, coding and testing providing the knowledge and introductory skills needed to successfully develop and test secure web applications.

The core level course is an important course to take if you wish to develop or rely upon web applications, or will have risk, or governance responsibilities in any organisation which uses or develops web applications i.e. just about everyone.

The extended level course is for security professionals or professional web developers and covers a wider range of vulnerabilities and in greater depth than the core level courses.

Extended course content for COMP6843 students will be covered in the extended lecture. COMP6443 students are welcome to attend the extended lecture if you are interested.

Core Content

- Reconnaissance
- Relevant Tooling Used in Industry
- Server-side attacks, such as SQL injection, Local File Inclusion, and Server-side Request Forgery
- Client-Side vulnerabilities, such as Cross Site Scripting
- Authentication
- Session Management
- Access Control and Privilege Escalation
- Common web service vulnerabilities
- Patching and remediation
- Secure web coding best practice
- Vulnerability reporting and professional communication
- Pen-testing in Industry

Extended Content

- Professional testing and assessment practices
- Advanced Asset Discovery and Reconnaissance
- Advanced Server-side Attacks such as XML External Entity Exploits
- Advanced Authentication Attacks such as attacks against OAuth and SAML
- Advanced Client-side Security Attacks and Defences

Course coverage is updated each year to reflect emerging vulnerabilities and practices.

Assessments

Item	About	Marks
Self-assessment Quiz	Distributed in week one to be done in your own time. It is designed to provide an insight into the expected knowledge for this course and is not accessible. If you have difficulty with the quiz, speak to your tutor.	0%
Fortnightly practical activities	Applying practical skills learnt in lectures/tut-labs to a series of real-world practical examples. Often these are completed by 'capturing a flag'. Students are encouraged to collaborate with other students, but all students must solve challenges and submit their work independently.	25%
Written assessments	Penetration testing type reports that incorporate a description of the vulnerabilities found, overview of exploits used, and remediation recommendations. The written reports are submitted in teams formed from your tutorial class.	25%
Practice Exam	Held in week 5, likely in the Tuesday lecture slot. All content from prior weeks is assessable, including fortnightly activities. Serves as a self-check on how you are performing in the course, and what to expect in the final exam.	10%
Final Exam	Held in the university exam period. This will be an online exam with more details closer to the date. The exam will include a practical	40%

Item	About	Marks
	component, which is best prepared for by doing fortnightly practical activities.	

Course weekly schedule

Week	Topics	Industry Lecturers
1	Topic 1 - How the web works/Reconnaissance	• Norman Yue • Abhijeth Dugginapeddi
2	Topic 2 - Authentication and authorisation	• Yunsar Jillani
3	Topic 2 - Authentication and authorisation	• Marina Levi
4	Topic 3 - Server Side attacks	• Yunsar Jillani • Abhijeth Dugginapeddi
5	Topic 3 - Server Side attacks	• David Jorm
6	Quiet Week	
7	Topic 4 - Client-side	• Marina Levi
8	Topic 4 - Client-side	• Varun Chandramohan
9	Topic 5 - DevSecOps	• Varun Chandramohan

Week	Topics	Industry Lecturers
10	Topic 5 - DevSecOps	• David Jorm

How to successfully approach this course

To get the most from UNSW's SECedu security courses you will need to engage in independent study and act as a self-directed learner. Simply attending lectures will not be sufficient to master the material or pass the course. You will need to devote considerable time to self-directed practice of the techniques we cover and also to read further on topics which interest you or which you do not fully understand. To achieve a credit level result, we expect you will spend 15 hours per week on this course.

Seek feedback from your friendly tutor and class peers constantly over the term and closely monitor yourself to make sure you are not falling behind. We will not force you to do the self-directed work and practice - but experience has shown that students who do not work hard at the course do not do well, and often express disappointment and regret later at the missed opportunity. (Since we have awesome lecturers and tutors here for you during the course - make sure you make full use of them and your time.)

Make sure you improve your time management skills if you do not feel you are strong in time management. That will also have benefits beyond this course in your future professional life. Seek advice and help from your tutor and/or from the university student services if you feel you need more development here.

Requirements

This course requires you to Bring Your Own Device. Even if you are attending a tutorial class on campus, CSE lab computers don't have the required software to perform exercises or assignments. Any laptop capable of running the software in the preparation activities should be sufficient, you do not need a super-fancy machine.

You should set up a Linux virtual machine on your personal or spare laptop. If you have difficulties in hosting the virtual machine, discuss this with the course staff as soon as possible and ensure you have been able to arrange satisfactory workable solutions before the census date.

Assumed Knowledge

You need to have taken and passed COMP6441 or 6841.

We expect you to already have or be prepared to teach yourself basic web programming skills such as covered in Web Applications Engineering - COMP9321.

Specifically, prior to commencing the course, students should have an understanding of how the web works, and basic scripting principles including:

- Familiarity with web technologies: HTML, CSS, JavaScript, Databases
- Moderate familiarity with at least one web development language like Golang, Java, Python, PHP, etc
- Basic knowledge of network and web related protocols (e.g. TCP/IP, UDP, HTTP, HTTPS)

Familiarity with the unix command line, scripting and basic automation via bash/python etc. will be helpful through the course.

Learning Outcomes

After completing COMP6443, you will have the skills of a security aware web developer:

- Understand how modern web applications work
- Be able to use secure coding practices to develop web applications
- Know the common security vulnerabilities that affect web applications and associated infrastructure
- Understand the principles of how to defend against these attacks
- Have an understanding of mobile application security principles

After completing COMP6843, you will have the web application skills of a security engineer:

- Understand how modern web applications work
- Be able to use secure coding practices to develop web applications
- Know common and more advanced security vulnerabilities that affect web applications and associated infrastructure
- Understand and be able to apply the principles of how to defend against these attacks
- Be a competent user of a core set of specialised security tools to assist in assessing the security of web applications

This course contributes to the development of the following graduate capabilities:

Graduate Capability	Acquired in
Scholars capable of independent and collaborative enquiry, rigorous in their analysis, critique and reflection, and able to innovate by applying their knowledge and skills to the solution of novel as well as routine problems	Lectures, Tutorial-labs, Activities and Assessments

Graduate Capability	Acquired in
Entrepreneurial leaders capable of initiating and embracing innovation and change, as well as engaging and enabling others to contribute to change	Lectures, Tutorial-Labs, team learning activities
Professionals capable of ethical, self-directed practice and independent lifelong learning	Lectures, Written and practical activities
Global citizens who are culturally adept and capable of respecting diversity and acting in a socially just and responsible way	Lectures, team learning activities

How the Course is Taught

6443 students enrol in the common lecture stream (3.5 hours/week), and one of the core stream tutorial-lab sessions (2 hours/week).

6843 students enrol in both the common lecture stream (3.5 hours/week), and the extended lecture stream (1 hour/week), and one of the extended stream tutorial-lab sessions (2 hours/week).

Lectures

Lecture are used to introduce students to theoretical and practical concepts and will include practical demonstrations. Most of the teaching is from industry experts who want to give back to the security community and are generously sharing their practical, specialised experience with you.

Lectures will mostly be conducted face-to-face with live-streaming on Echo360. A recording will be accessible from the course Moodle page. Some of the lectures will be delivered fully online via Zoom. We will identify the online lectures in the Timetable section on the OpenLearning course website. We strongly recommend that you attend the lectures in person when available.

Tutorial-labs

The tutorial-labs are facilitated small group classes to allow students to further develop and understand lecture concepts through collaborative learning and experienced instruction. Part of the time will be devoted to solving problems and discussing solutions related to lecture topics and past weeks' assessments and activities. The

remaining time will be used to discuss topics relevant to the current assessment. Any assessment work not completed during the 2-hour tutorial-lab time you should (of course) complete in your own managed study time.

In-term assessments

Students are expected to apply and consolidate the knowledge they have gained by carrying out weekly practical exercises and written assessments.

COMP6843 has additional assignments on advanced exploitation skills and on more difficult web vulnerabilities.

You may be penalised 10% per day of the marks available for an assessment task if you submit it after the due date, unless you have an approved extension through Special Consideration [https://www.student.unsw.edu.au/special-consideration].

Team Work

Where assessments are for materials produced by teams of more than one student all team members will receive the same mark. In cases where students can document outstanding teamwork additional bonus marks may be awarded to individual team members. An example of outstanding teamwork is if you notice a problem in your team and you make serious and thoughtful attempts to address and fix the problem (including effective approaches to try to re-include absent team members, finding out and trying to address any underlying issues which are leading to members not engaging, addressing and fixing concerns the team is having, and plan for contingencies when that seems needed) Note there are typically NOT any extra marks for doing it all yourself, that is rarely the best way to deal with team problems. Use your tutor and any mentors you respect as a source of advice about how best to fix team problems - and make sure you document your plans and strategies as part of your professional development as well as to support a case for teamwork marks.

Marks

Course results and exam marks will be scaled if necessary, to keep the standard of the different grade levels consistent from year to year and between the security engineering courses. In cases where the overall result for the teamwork assessment items significantly exceeds the individual (non-team) assessment items the teamwork results will be capped at the level of the individual results and you may be called in for an interview to explain the difference. In significant cases you may be offered further practical individual assessment activity to replace your team results and you will not be awarded a pass in the course unless you clearly demonstrate pass level ability in that work.

Identified Work

We use assessment feedback as a way of your facilitator getting to know you and the areas in which you need help. Hence assignment work is not marked anonymously. Contact the course administrator or lecturers if you have any individual concerns with this approach. Wherever possible we share student work as a way of developing the entire cohort, if you do not wish to be identified in any of your work which is shared contact the course administrator or lecturers and discuss it with them BEFORE submitting the work.

Student Conduct

UNSW has genuine and serious commitment to fostering a culture of learning informed by academic integrity. All UNSW staff and students have a responsibility to adhere to this principle of academic integrity.

Plagiarism

Plagiarism is using the words or ideas of others and passing them off as your own. This includes something as simple as using a phrase copied from the internet in something you submit but not clearly acknowledging that it is a quote and where it came from. Be careful – rules at UNSW may well be different from what you learned at your high school or in other institutions or countries. For example, simply giving a list of references at the end of a piece of submitted work but not at the same time making it clear which phrases came from which work is not sufficient and would still constitute plagiarism.

Plagiarism undermines academic integrity and is not tolerated at UNSW. Punishment can be extremely severe so make sure you understand what constitutes plagiarism at UNSW by reading the linked materials:

- UNSW's policy regarding academic honesty and plagiarism
- Student Code Policy Plagiarism Policy Statement Plagiarism Procedure
- Student Misconduct Procedure

Good Faith Policy

In all our security courses we expect an extremely high standard of scrupulous professionalism from our students. You must not do anything which could bring you, other students, tutors, staff, guest lecturers, SECedu, UNSW, Australia or the profession into disrepute. Otherwise this could endanger the existence of security engineering education at UNSW and perhaps damage the professional reputations of yourself and others. So for example:

Don't break any laws or university rules (even stupid ones), encourage anyone to break any laws or university rules, hack anything or anyone, damage or try to access UNSW systems in any manner other than normally logging into things to which you already have legitimate access. Don't brute force anything, pen test anything, socially engineer anyone, or divulge any private information or information about vulnerabilities

without first obtaining written consent. Respect the property of others and the university. Always abide by the law and university regulations Be considerate of others to ensure everyone has an equal learning experience. Always ensure that you have appropriate written permission before performing a security test on a system.

These are just examples, we won't give an exhaustive list as I bet you could figure out a way to satisfy the strict letter of the list but still do something which could put the course into jeopardy – so instead try to be as careful and ethical as you can and if you have any questions or even the slightest doubt about possible courses of actions ask and check first with the course staff before doing anything.

Failure to adhere to this policy may result in an academic penalty, automatic failure from the course, and/or a charge or Academic Misconduct on your transcript and being excluded from the university. So please take it very seriously.

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.

Changes Made in Response to MyExperience Feedback

Based on some constructive feedback received from our students last year, we made some changes in the current course offering. In our last year course (i.e., 2021T2), the first report was due in Week 7, which resulted in giving late feedback to students. In our current offering, the first report is due in Week 5, thereby giving a couple of more weeks to students to get the feedback from their tutors and implement them in the second report. We also aim to introduce the profiles of all our lecturers in our introductory class so that students can plan their meetup accordingly. Based on difference in the technicality level, we have also balanced the level of difficulties in CTF challenges across COMP6443 and COMP6843 so that students from both courses are equally benefited. We will also provide CTF challenges solutions to students after reports submissions. Finally, the marks distribution for practical activities (i.e., CTF challenges) will be clearly provided to students via tutors.

Textbooks and Reference Books

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

You, The Future

We are proud of our former students, they are awesome, and go on to do good things and be good people. Indeed some of the industry guest lecturers in UNSW SECedu courses are former UNSW security students. So please stay in touch after you have graduated and let us know your achievements and what you are doing. It makes us happy and we are proud to brag about you.

Please do thank the returning and new guest lecturers and let them know how much you appreciate their effort and care in giving up so much time to help you. They go to considerable trouble to do this and they do it because they think it is the right thing to do to grow the profession and to help those coming after them.

After you graduate please consider giving back (well, paying forward really) and coming back to help future students once you are an industry practitioner. The help former students give future students is quite moving and changes lives.

Also, even sooner than that, after you have finished this course, if you enjoyed it, then let your tutor know and we will consider you as a staff member for the next offering of the course. Teaching others is very rewarding, gives you great professional skills, makes you more connected in the profession and, weirdly enough, helps you master the material of the course to a level far beyond the level you attained when you did it as a student. We don't just look for results when selecting tutors and course staff. The lecturers are the domain experts, not the tutors. In selecting tutors we mainly look for communication ability, kindness, an interest in developing leadership skills, a sense of fun, and a love for the course material.