Web Application Security & Testing - COMP6443

Extended Web Application Security & Testing - COMP6843

Course Outline 2019T1

These two courses run in an overlapping mode. All students share a set of common 6443 activities and assessments, 6843 students however have additional activities and assessments related to penetration testing in lieu of construction assignments 6443 students are expected to complete. Except where indicated all the information below relates to students in both courses.

Course Staff

Course Convenor: Prof Richard Buckland

Lecturers and Teaching Staff

- Norman Yue
- Abhijeth Dugginapeddi
- Sean Yeoh
- John Cramb

Course Admin: Zain Afzal

Contact Us

- Speak with the lecturers at and after lectures
- Speak with your tutor at tutorials
- Chat with us and your classmates on the course forum
- Confidential questions to Zain at: cs6443@cse.unsw.edu.au
- General enquiries about Security Engineering major to Anatoli at: SECedu@unsw.edu.au

Classes

6443 students enrol in the common 3-hour lecture stream, and one of the 2-hour core stream tutorial-lab sessions.

6843 students enrol in both the common 3-hour lecture stream and the 2-hour extended lecture stream, and one of the extended 2-hour tutorial-lab sessions.

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 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 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 too if they are interested.

Core content

- Reconnaissance
- Relevant Tooling Used in Industry
- Server-side attacks, such as SQL injection and Local File Inclusion
- 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 also includes

- 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 XSS such as Sandbox Escape and XSS against bots
- Same Origin Policy/Content Security Policy Bypasses
- DNS Rebinding
- Advanced Injection such as Template and Email injection
- Web Cache Poisoning
- Server-Side Request Forgery (SSRF)
- Cloud Platform Exploitation such as AWS exploits
- Bug Bounties

Course coverage will be updated over time to reflect emerging vulnerabilities and practices.

Assessment

	6843	**6443**
Break Wargames	30	30
Patch Wargames	n/a	20
Extended Break Wargames	20	n/a
Midsem Exam	10	10
Theory Exam	10	10
Prac Exam	30	30
Bonus	6	6

Assessment Activities

Break Wargames
Involves applying practical skills learnt in lectures/tute-labs to exploit a set of vulnerabilities.
Homework assignments done in pairs released approximately fortnightly.

Construction Wargames Involves receiving a vulnerable web application and patching it to be secure.
Homework assignments done in pairs and released approximately fortnightly.

Extend Break Wargames Involves applying practical skills learnt in extended lectures/tute-labs to exploit a set of vulnerabilities as well as attempting to exploit more advanced vulnerabilities learnt about in the standard course.
Homework assignments done in pairs released approximately fortnightly. Students may complete the homework assignments individually on approval by the lecturer.

Mid-semester Practice Exam Held in the Monday lecture time slot in week 4. Based

on the material taught up till that time. If your result in your final exams exceeds the mark you get in this practice exam, or if you miss this practice exam, then the practice exam mark will be replaced with your result in the final exams.

Final Theory Exam

Written short answer and multiple-choice exam held in the Monday lecture timeslot in the last few weeks of the course. Largely based on the tutorial-lab classes and guest lectures. The date of the exam will be advised in the first lecture.

Final Practical Exam

Two x 12 hour take home practical exams, held in the exam period. Largely based on the Wargames.

Optional Bonus Activities

- Up to 4 bonus marks given for doing something self-directed and impressive which develops yourself over the course of the semester such as participating in bug bounties or building a tool or resource for others. Discuss your proposed “impressive” project in advance with your tutor and seek feedback over the semester. Marks are given for documenting the progress and reflection.
- Up to 2 bonus marks given for undertaking the optional lab presentations - your lab facilitator will discuss this.

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. Attending lectures alone will not be sufficient to pass the course. You will need to devote considerable practice in your own time to all the techniques we cover and 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 lab facilitator and class peers constantly over the semester and closely monitor yourself to make sure you are not falling behind. We treat you like adults and 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 on at the missed opportunity. (Since we have awesome lab facilitators and speakers 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 help from your lab facilitator and from the university services if you feel you need more development here.

Requirements

This course requires you to Bring Your Own Device. CSE lab computers won't have the required software to perform exercises or assignments. Any laptop capable of running the software in the pre-course preparation activities (Week 0 Activity) should be sufficient, you do not need a super-fancy machine.

if you have difficulties in arranging having your own device for assignments, tutorial-labs, and the exams discuss and this with the course staff as soon as possible and ensure you have been able to arrange satisfactory workable solution before the census date.

Assumed Knowledge

You need to have taken and passed COMP6441 or COMP6841 or COMP3441 or COMP9321. We expect you to have or be prepared to teach yourself basic web programming skills such as are taught in Web Applications Engineering - COMP9321

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

- Web technologies: HTML, CSS, JavaScript, Databases, Server-side Scripting (e.g. PHP)
- Moderate familiarity with at least one web development language like Java, Python, PHP, etc

- Basic knowledge of network and web related protocols (e.g. TCP/IP, UDP, HTTP, HTTPS)

Although not strictly needed familiarity with the unix command line, scripting and basic automation via bash/python etc. will be helpful through the course.

Course Learning Outcomes

After completing these course, you will:

- 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 and how companies can implement a Secure Development Life Cycle (SDLC) to mitigate potential vulnerabilities
- Have an understanding of mobile application security principles
- Be a competent user of a core set of specialised security tools to assist in assessing the security of web applications

These courses contribute to the following Graduate Capabilities:

- 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
- Professionals, capable of ethical, self-directed practice and independent lifelong learning;
- Entrepreneurial leaders, capable of initiating and embracing innovation and change, as well as engaging and enabling others to contribute to change
- Global citizens, who are culturally adept and capable of respecting diversity and acting in a socially just and responsible way

Week 0 – DO THIS BEFORE THE FIRST LECTURE

On the basis of past suggestions from students this year we have put together set up activities for you to do BEFORE week 1 of the course. These will get you familiar with

relevant tool sets and get your machine set up ready for the activities in week 1.

The week 0 activities can be found on webcms. A copy is available at https://www.cse.unsw.edu.au/~z5059449/cs6443/week0/Getting_Started.html

Go there and get started at once – it should be fun and give you a taste of the things to come.

How the Course is Taught

The core and extended streams COMP6443/6843 are taught in parallel. The core lectures are common for all students. Students doing Extended Web Application Security and Testing (COMP6843) also attend an extra 2-hour extended lecture. All students have weekly 2-hour tutorial-lab sessions.

Lectures are used to introduce students to theoretical and practical concepts, and will include live and recorded demonstrations. There will be guest lecturers coming in from industry to share practical specialised experience with the students.

We are fortunate to have experienced experts and industry practitioners contributing to lectures and other course activities, and that they speak freely and frankly about relevant experiences they have had. They have asked that this not be recorded (for confidentiality and so they can speak freely and not self censor). So in this course you may not record any lectures or course activities without the written advance consent of the lecturers / other people being recorded.

We will make our best efforts to release our own edited lecture recordings within a few weeks of each lecture but the delay and uncertainty about when they will be released and what they be able to include means they are not a perfect replacement for attending lectures, or nearly as good or fun. Former students strongly recommend attending all classes.

Tutorial-labs: 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' assignments. The remaining time will be used to discuss topics relevant to the current assignment. Any assignment work not completed during the 2-hour tutorial-lab time you should (of course) complete with

your assignment partner in your own managed study time for these courses.

Assignments: Students are expected to apply the knowledge gained in practical assignments known as war games. These will vary in difficulty and will cover various aspects of Web Application Security. Additionally, COMP6443 students will be asked to create their own Web Applications to develop their secure coding practice skills.

Students will work in facilitator selected pairs to complete these assignments, you will change partners every two weeks.

For the extended course it is assumed that students are already able to build and secure simple web apps, and therefore COMP6843 has additional assignments on advanced exploitation skills and on more difficult web vulnerabilities.

Late assignments will be subject to a late penalty.

Supplementary exams will only be awarded in well justified cases. They will not be awarded if your reason for not sitting the final exam was for holiday travel (!). Read the School policy for *Special Consideration*.

There will only be one supplementary exam. If you miss it you will not be awarded another. So do not plan overseas travel at the end of the exam period if there is any chance you may wish to sit a supplementary exam. It is up to you to contact the school office and/or website and find the date of the supplementary exam and keep it free (the date is usually set centrally by the school not by the course staff) If you think you might be eligible for the supplementary exam hold yourself ready to sit it – sometimes people are awarded entry to the supplementary exam at the last minute and saying “I didn’t know if I would be awarded it so I didn’t study for it” is not a valid reason for special treatment.

Default late penalty: Unless otherwise specified for assessment submissions in this course the late penalty will be:

- a cap of 90% for submissions up to 24 hours late, a cap of 75% for submissions up to 48 hours late, and a cap of 50% for submissions up to 3 days late. Submission more than 3 days late will receive 0 and not be marked.

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. For example if there is a problem in a team and serious and thoughtful attempts are made to address the problem (including effective approaches to try to include absent team members, address and fix concerns the team is having, and plan for contingencies when that seems needed) Note there are not typically any extra marks for doing it all yourself, that is rarely the best way to deal with team problems. Use your facilitator 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.

Marks

Course 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 developing the entire cohort, if you do not which 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 (even stupid ones), encourage anyone to break any laws, hack anything or anyone, damage or try to access UNSW systems in any manner other than normally logging into thing 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. 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 just 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 check 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.

Course Evaluation and Development

These courses are still relatively new, and we strongly encourage students to actively provide feedback about the course's progress. Each tutorial-lab class will elect a student representative – give your feedback to them and they will pass it onto the course staff anonymously. We'll also run some feedback sessions over the course where you can give feedback and suggestions. Many of the good things in the course now have come from students giving great suggestions in the past so do pass on your thoughts we take them seriously and they make a difference.

These courses will also be evaluated by UNSW's myExperience survey and feedback program at the end of the trimester. It's annoying but it actually helps us a lot if you fill it in as it's pretty much the main feedback that the rest of the university administration looks at and good feedback helps us survive and grow.

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 many of the industry guest lecturers are former security students. So please stay in touch after you have gone 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 current returning guest lecturers and let them know how much you appreciated their effort and care in coming back 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 yourself 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 facilitator 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 facilitators and course staff. The lecturers are the experts, not the facilitators. We mainly look for communication ability, kindness, an interest in developing leadership skills, a sense of fun, and a love for the course material.