THIS DOCUMENT IS A DRAFT, AND MAY BE SUBJECT TO CHANGE.

COMP6443
Web Application Security and Testing

Semester 1, 2017
6 UoC — offered S1 — for UG + PGC

Course Aims and Outcomes

Web applications are currently the predominant source of software vulnerabilities exploited 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.

This course covers

- OWASP vulnerabilities
- cross site scripting
- browser security model and weaknesses
- Injection attacks
- DNS
- Man in the middle
- Data leakage
- Spoofing
- Ul 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 Learning Outcomes

After completing this course, you will

- understand how modern web applications work;
- be able to assess the security of a web application using white/grey/black-box approaches;
- know the many common pitfalls and security vulnerabilities that affect web applications and associated infrastructure;
- understand how to defend against these attacks and how companies can implement a Secure Development Life Cycle (SDLC) to mitigate potential vulnerabilities;
- have a basic understanding of mobile application security concerns; and
- have practical knowledge of specialised security tools which assist in assessing the security of a web application.

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

Assumed Knowledge

This course has COMP3441, COMP9441, COMP6441, or COMP6841 as its formal prerequisite.

Students should have an understanding of how the web works, and the basics of the following subjects:

1. Web technologies: HTML, CSS, JavaScript, Databases, Server-side Scripting (e.g. PHP)
2. Moderate familiarity with at least one web development language like Java, .NET, PHP, etc.
3. Basics of networking knowledge

Course Staff

Lecturer-in-Charge
Dr Roland Wen (https://www.openlearning.com/u/roland.wen)

Lecturers and Teaching Staff
Norman Yue (https://www.openlearning.com/u/ilikeplatypodes)
Abhijeth Dugginapeddi (https://www.openlearning.com/u/abhijeth)
Brendan Hopper (https://www.openlearning.com/u/dzhkh)
Fionnbharr Davies (https://www.openlearning.com/u/thoth)

Course Convenor
Prof Richard Buckland (https://www.openlearning.com/u/richard.buckland)

Course Admin
Jashank Jeremy (https://www.openlearning.com/u/jashankj)

for confidential course enquiries, email
cs6443 at cse dot unsw dot edu dot au

Teaching Strategies

Lectures will be 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.

Students will be expected to apply the knowledge gained through lectures in practical environments known as **war games**. These can vary in complexity from basic examples up to an entire virtual machine that you need to compromise. Most of the war games will be purely for learning but others will assessed and make up a percentage of your final mark.

Assessment

- **Coursework**: practical homework exercises done in groups. Weekly; worth 40%.
- **Community involvement**: portfolio demonstrating engagement with and contributions to the security community --- in this course, at UNSW and in industry. Throughout the semester; worth 10%.
- **Final Examination**: a primarily practical (though with some theory) examination. During the university's exam period; worth 50%.
- **Bonus**: portfolio of bug bounties verified by third party or similar. Throughout the semester; worth up to 5%.

Academic Honesty and Plagiarism

UNSW has an ongoing 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 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.

If you haven't done so yet, please take the time to read the full text of UNSW's policy regarding academic honesty and plagiarism (https://student.unsw.edu.au/plagiarism).

The pages below describe the policies and procedures in more detail:

- Student Code Policy (https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf)
- Plagiarism Policy Statement (https://www.gs.unsw.edu.au/policy/documents/plagiarismpolicy.pdf)
- Plagiarism Procedure (https://www.gs.unsw.edu.au/policy/documents/plagiarismprocedure.pdf)
- Student Misconduct Procedure (https://www.gs.unsw.edu.au/policy/documents/studentmisconductprocedures.pdf)

Good Faith Policy

This course has a “Good Faith Policy”. This means we expect you to act in good faith at all times. We expect you to be a good citizen.

- **Do not** invade, alter or damage the property of others including the university, invade the privacy of others.
- **Do not** break any laws or regulations.
- **Do not** annoy other people.
- **Do not** deprive others of access to resources, breach or weaken the security of any system, or do or omit to do anything else which you know or suspect we would not be happy about.

Furthermore, you are not to do anything which appears *OK* by a loophole or a strict interpretation of “the letter of the law” but which is not consistent with the spirit.

Basically, you must not act in any way so as to bring disrepute to the reputation of the course, the course staff, fellow students, the school, the university, or the ICT profession.

If you are unsure, ask!

If, in our sole discretion, we feel you have violated the Good Faith Policy you will be awarded 0 Fail for the course. Further penalties may apply also depending on the nature and severity of the violation. Students who have violated the Good Faith Policy may not be permitted to re-enrol in future offerings of the course.

Students who are found (or who have previously been found) guilty of academic or computer related misconduct or any other activity in a way which which casts doubt on their ability or willingness to comply with the Good Faith Policy will be unenrolled and will be not permitted to re-enroll in future offerings of the course. If you have ever been found guilty of such an activity you must disclose it to the lecturer in writing immediately.

Course Evaluation and Development

This is the first offering of this course. We strongly encourage students to actively provide feedback about the course's progress.

This course will be evaluated by UNSW's myExperience program. You'll receive an email to your student email address with instructions on completing this; we'll also (endeavour to) send out a notification.

This course will also be evaluated by the CSE Student Representatives' mid-session Course Survey.