COMP6443 25T1 - Week 1

A Brief Web History

TrashPanda, 18th Feb 2025

What Will I Get From This Course?

L.J.H.S.!

https://livelectures.quoccacorp.com/welcome

First person to make a popup with “You’ve been owned by <zid>” gets a prize.

Expert External Hackers

With an Understanding of Networks

- Identify vulnerabilities, by manual testing and automated tooling, in web applications and parts of their infrastructure.
- Exploit said vulnerabilities, both manually and with self-written scripts.
- Understand publicly available exploitation tools, their risks, and how to use them appropriately.
- Communicate the technical details of a particular vulnerability and accompanying exploits.
- Convince non-technical stakeholders of the risk and significance of a vulnerability.

Admin

Good Faith Policy

Don’t Be A Dick

- Don’t interfere with people’s learning
- Don’t DoS any systems
- Don’t drop tables
- Don’t run scripts if you’re not certain about what they do

- Don’t be a dick.

Scope

No fr, this is important.

- You are NOT allowed to attack:
  - UNSW Infrastructure not listed explicitly within the permitted scope above
    - *.unsw.edu.au
    - WebCMS
    - Ed
    - UNSW's Moodle

- ctfd.quoccabank.com
- questions.quoccabank.com
- *.internal.quoccabank.com
- Any exam pages

- This includes passive information. If you find something out of scope, we don't want to hear about it.
- Blacklisting overwrites whitelisting rules.
- Full scope, with updates through the term, is found on WebCMS. - https://webcms3.cse.unsw.edu.au/COMP6443/25T1/resources/107959

Scope

No fr, this is important.

- You ARE allowed to attack:
    - *.quoccabank.com
        - Unless explicitly forbidden
    - Anything with a bug bountry program
    - Anything you have explicit written permission from the owner and maintainer of the system

Assessments

“100 sympathy marks pls 🥺”

- Final Exam - 50%
  - During exam period
- Report 1 - 15%
  - Due in week 5
- Report 2 - 15%
  - Due in week 11

- Weekly Activities - 20%
  - Assessed through the term
- Midterm Exam - not assessed
- All the details can be seen on WebCMS. We’ll talk more as the assessments approach.

Course Schedule

When will things be due?

- Topic Challenges: 12pm (midday) on the...
  - Topic 1: 4th of March 2025 (Tuesday, Week 3)
  - Topic 2: 11th of March 2025 (Tuesday, Week 4)
  - Topic 3: 1st of April 2025 (Tuesday, Week 7)
  - Topic 4: 15th of April 2025 (Tuesday, Week 9)
  - Topic 5: 29th of April 2025 (Tuesday, Week 11)
  - Topic 6: 29th of April 2025 (Tuesday, Week 11)

- Report 1: 12pm, 1st of April (Tuesday, Week 7)
- Report 2: 12pm, 29th of April (Tuesday, Week 11)

- Midterm: 6pm-7pm, 18th of March (Tuesday, Week 5)
- Final: TBD (but we're hoping it's a Tuesday)

Course Schedule

When will things be due?

- Tuesday.
- Is it Tuesday? Oh heck, something is due.
- When is this due? Idk, but it’ll defs be a Tuesday.

Weekly Schedule

What do I need to attend?

- Base course (COMP6443):
  - Tuesday lecture - 6pm-8pm
  - Wednesday Lecture - 4pm-6pm
  - One of any tutorials through the week
    - (Preferably the one in which you're enrolled)

- Extended course (COMP6843):
  - Tuesday lecture - 6pm-8pm
  - Tuesday Extended lecture - 8pm-9pm
  - Wednesday Lecture - 4pm-6pm
  - One of any tutorials through the week
    - (preferably an extended)
    - (Preferably the one in which you're enrolled)

Course Resources

If in doubt, check WebCMS

- Moodle
  - This is where you can get access to Ed and where things will be submitted such as the reports and the final exam
- WebCMS
  - https://webcms3.cse.unsw.edu.au/COMP6443/25T1/
  - This is the course website. This is where all announcements will be posted. If you don't have access to this, you need to let us know.
- EdStem
  - https://edstem.org/au/join/gSd8uM
  - Here's where you can ask questions :) (we listened to you from 6841)
- CTFd
  - Https://ctfd.quoccacorp.com

Course Contacts

Who do I ask?

- Step 1: Ask your peers! There are some very brilliant people in this course who will be happy to help you and nerd out over some sick vulns

- Step 2: Ask your tutor - or any tutor :D All of them will have an answer - even if the answer is "I'll go ask X"

- Step 3: Ask on Ed

- Step 4: Ask Hamish or me in the lectures

- Step 5: email the course account on cs6443@unsw.edu.au

- **Step 0:** If it is sensitive or involves personal information such as ELPs or issues with groups, bypass all this and email either the class account or me directly on kristian.mansfield@unsw.edu.au

Lecture Questions

Pls ask 😭

- https://questions.quoccacorp.com

The MOST IMPORTANT Part of the Course!!!

Memes.

Some Important Knowledge

Terminology

There's probably more but we'll enounter that through the course

- TCP
  - Packets will be delivered in order and confirmation when packets are delivered
  - We don't care about TCP/IP or anything about how the messages are going across, just that messages are received.
- Client/Server dynamic
  - Client sends requests, server sends responses
    - This dynamic is inverted in some cases of remote shells, but we'll discuss that when we get there.

How the internet works

COMP3331 in one slide

- DNS
- Router & Modem
- Firewall
- ISP
- Certificates

Servers Are Magic

What is a Proxy?

- When people say VPN, they usually mean proxy.

Setting up

Important Resources

You'll want all of these but feel free to use an alternative if you have one

- Burp.
- Python - because no one wants to write C or Bash to script things
- A hosting platform
  - requestbin is nice but not reliable

Let’s Do It Live!

Step 1:
import sockets…

Step 2:
Get a resource

Step 3:
HTML

Step 4:
Status Codes

Step 6:
Versions and Headers

Step 7:
What else can I do with requests?