Final Exam - COMP6443/COMP6843 2020s2

Exam Info

Format

The exam 'paper' is listed below. There are two sections - the short answer, and the long answer section. The short answer has 5 smaller challenges, and the long answer section has 1 larger app.

Both COMP6443/6843 students should attempt all questions. To assist with solving challenges, we've included the number of flags for each challenge, and their relative difficulty (trivial/easy/medium/hard/extremely hard). CTFd points associated with each difficulty level are listed as following:

- **trivial**: 8
- **easy**: 10
- **medium**: 20
- **hard**: 30
- **extremely hard**: 50

CTFd points for flags labeled with two difficulty levels (e.g., medium/hard) is the arithematic mean of the associated points listed above. For instance, medium/hard flag corresponds to 25 points.

CTFd marks are nominal only and do not reflect your final mark. We will use a formula similar to midsem and fortnightly challenges to scale your final mark (considering both CTFd points and solving statistics). We reserve the rights to modify the formula or apply further scaling (this is usually to scale up your marks).

Some harder flags are not designed for core students, so don't feel disheartened if you can't get them all. Under some multi-flag questions we indicate what would be a reasonable number of flags to acheive. Remember, marks are scaled based on cohort performance, so if you've been performing well in the semester, you will perform well in this exam.

Unless otherwise specified, flags will be of the format `COMP6443FINAL{......}`

Submission

Flags

Submit flags as you go to https://ctfd.quoccabank.com (https://ctfd.quoccabank.com).

Caution: All flags must be submitted before 21/08/20 at 5pm (AEST).

Write-up

You will be required to submit a write up of your flags - this is a simple paragraph that explains the steps used to obtain the flag. This will be verified to ensure flags were obtained legitimately. It doesn't have to be long - just one or two sentences followed by your payload should be good enough. Please clearly mark the question for each answer.

Answers without an accompanying write-up will be considered invalid.

You should submit this write up as a PDF via give before 21/08/20 at 5:15pm (AEST). Please submit multiple times to save your work. We will use your last submission as your write-up.

Submit it by SSH-ing to CSE server or VNC-ing into VLAB and run (both COMP6443/6843 students)

```
give cs6443 exam writeup.pdf
```

Double check your submission is correct by running (both COMP6443/6843 students)

```
6443 classrun check exam
```

Please note that give's web interface might not be as stable as its CLI client and therefore we recommend using **`give`** command directly. We will announce alternative submission methods if CSE's login servers or NFS server goes down. But we won't consider it an issue if give's web interface or webcms3 goes down without affecting directly using **`give`** command.

Please email us if you have any issues with using **`give`**.

Tools

Below are some tools that you might find useful (we are not affiliated with any of them):

- requestbin.com (https://requestbin.com)
- google.com (https://google.com) or your favorite search engine
- A Linux server. While you don't have to have a linux server to do the exam, we feel that having one might be convenient. You can get $50 USD GCP credit for free here (https://google.secure.force.com/GCPEDU?cid=iu2JTcGvQ9j9pJjpeIgFWX38JqRySJ2Tf7Yhwsu9JdegXoLQi7nbhH%2FQ6E0pAp9V). DigitalOcean offers $50 for students via GitHub Education Pack (https://education.github.com/pack). Some other common choices are AWS, Azure, Linode, Vultr, Aliyun, etc.
- Browser DevTool
- Python or your favorite scripting language

Exam Rules

- This exam is 'open-internet', where you have free access to read and download from the web.
- You **MUST NOT** post/communicate to the internet; including but not limited to sending email, Slack, Facebook Messenger, Whatsapp, Discord, etc.
- You **ARE** permitted to email the course account cs6443@cse.unsw.edu.au with any questions or queries.
- Any tool that automatically generates payloads is banned (including but not limited to SQLMap). An exception of this rule is you can use the tool if you wrote the tool yourself.
- Online brute-forcing (including but not limited to subdomain brute-forcing, sub-directory brute-forcing, password brute-forcing) is not permitted during the exam and is will not help you getting any flag. We have logging in place to detect this so please don't do it :) However, some challenges might have weak credentials (admin:admin type) or default credentials that's doable without the need of a dictionary.
- However, for some challenges, you might find it helpful to automate sending requests (different from brute-forcing against a dictionary. This is where you have a "smarter algorithm" to get the data you want) to the server with a short script. Please make sure your script makes requests at a rate lower than 10 QPS (queries per second) to make sure you won't get rate-limited by CTFProxy. Hint: binary-search has O(log n) time complexity.
- For some challenges, you might find it helpful to run an offline brute-forcing script (compute-intensive script locally on your computer/server without sending any outbound requests). This usually takes a few seconds at most. If it's taking longer

than 1 minute, it's not intended to be solved this way and you're going down a wrong path.

- Note that CTFd marks are nominal only and do not reflect your final mark - we will scale all results for fairness, so don't worry - just try your hardest!

Caution: Please do not discuss the paper until after 25/08/20 at 6pm (AEST).

Challenge Authentication Infra

The same mTLS-based authentication system that was used throughout the term is used for the exam. The first time you visit any new QuoccaBank subdomain, your browser will prompt you to choose your certificate. Whenever this happens, just click "OK". Unfortunately due to how browsers work, if you accidentally clicked "Cancel", you won't be able to access that domain name until you restart your browser process (entire OS process, not just a tab/window). Please note that some challenges may make API requests to a separate backend endpoint on a different subdomain and might prompt you to choose your certificate again.

If something goes wrong

- **For updates mid-way through exam**: We will post on Open Learning exam page (https://www.openlearning.com/unswcourses/courses/webapp-security/exam/), WebCMS (https://webcms3.cse.unsw.edu.au/COMP6443/20T2/) and in the Updates section (#updates) below.
- **If you have questions about the exam:** Email cs6443@cse.unsw.edu.au (mailto:cs6443@cse.unsw.edu.au) . Do not post in slack.
- **If there are outages**: We will post to all the above places with details.
- **If you have no internet**: please message 0402683020. Please write the number down now!

Updates

- None yet!

Section A

Question 1

qasa.quoccabank.com (https://qasa.quoccabank.com)

There are 4 flags to find:

- 4 x trivial recon flags

Question 2

pds.quoccabank.com (https://pds.quoccabank.com)

There are 7 flags to find:

- 1 x trivial recon flag
- 6 x easy flags

We don't expect you to find all flags. > 4 is a good effort.

Question 3

products.quoccabank.com (https://products.quoccabank.com)

There is 1 flag to find:

- 1 x medium flag

Question 4

logmein.quoccabank.com (https://logmein.quoccabank.com)

There are 3 flags to find:

- 1 x trivial flag
- 1 x easy flag
- 1 x medium flag

Question 5

poem-portal.quoccabank.com (https://poem-portal.quoccabank.com)

Note: This challenge requires recon outside of *.quoccabank.com. This is recon ONLY and you should NOT use any offensive techiques outside of *.quoccabank.com

There are 5 flags to find:

- 1 x trivial recon flag
- 2 x easy recon flags*^
- 1 x medium recon flag^
- 1 x medium/hard flag~

* These flags are of format `COMP6443{...}`

^ These flags are found outside of `*.quoccabank.com` scope

~ These flags require research outside of `*.quoccabank.com` scope

We don't expect you to find all flags. 3-4 flags is a good effort.

Section B

QuoccaOS

qos.quoccabank.com (https://qos.quoccabank.com)

There are 17 flags to find:

QOS - Homepage & Login

- 1 x trivial flag
- 1 x easy/medium flag
- 2 x medium flags
- 1 x medium/hard flag

QOS - Infra & other areas

- 1 x easy/medium flag
- 2 x medium flags

QOS - Tic-tac-toe

- 1 x easy flag
- 1 x medium flag
- 1 x hard flag
- 1 x extremely hard flag

QOS - Profile

- 1 x easy flag
- 1 x medium flag
- 1 x medium/hard flag

QOS - Handbooks

- 1 x medium flag (handbook v1)
- 1 x hard flag (handbook v2)

We don't expect you to find all flags. Finding 3-5 flags is a good effort for core students. More for extended students.

Found a problem? Email cs6443@cse.unsw.edu.au