# CS2107 Assignment 2

Last Updated: 21 October 2021

# Introduction

This assignment takes the form of an information security capture-the-flag (CTF) style competition. In a CTF, participants solve problems involving security weaknesses to bypass defences to obtain a sensitive piece of information called the `"flag"`.

In this assignment, participants are exposed to some of the common skills required to play in these competitions. When using the Assignment Platform, do not change your username. For password reset, it may take up to 5 working days so do use a secure yet memorable password.

Note that, for the assignment marking purposes, you additionally need to submit your write up to LumiNUS before the given deadline. This writeup should sufficiently share the approach that you took in solving every problem. You can refer to the "Rules and Guidelines" section for the instructions on submitting your write up and other supporting files.

## Acknowledgements

This assignment is a collective work of present and past teaching assistants, including Chan Jian Hao (AY 21/22), Ye Guoquan (AY 21/22), Debbie Tan (AY 20/21), Jaryl Loh(AY 20/21, AY 21/22), Wen Junhua(AY 20/21), Daniel Lim (AY 20/21), Chenglong (AY 19/20), Shi Rong (AY 17/18, AY 19/20), Glenice Tan (AY 19/20, AY 18/19), Ngo Wei Lin (AY19/20, AY 18/19), Lee Yu Choy (AY20/21, AY19/20, AY 18/19, AY 17/18), Nikolas Tay (AY 16/17) and Jeremy Heng (AY 16/17).

## Grading Scheme and Due Date

This is an individual assignment. You are allowed to post questions on the LumiNUS forum but ensure that the questions do not ask for the solution.
Additionally, do not post the answers to the challenges.

This assignment is worth 15% of the grade for the entire module. Assignment 2 is divided into the following sections:

1. Section A: Warmup - 8 Points
2. Section B: Network - 10 Points
3. Section C: Web - 60 points
4. Section D: Binary - 72 points
5. Section F: Bonus (Optional) - 10 points

The maximum number of points that can be obtained in this assignment is 150. The bonus challenges are optional, and are outside the scope of the module and are meant as self exploratory challenges for the curious. Regardless, you are awarded points if you solve them. Note that all your assignment marks and bonus marks obtained are to be capped at the 25 total marks possible for the Assignment assessment component of the module.

The assignment is due **17 Nov 2021, 2359 HRS**. Score penalties will apply for late submissions:

- Late up to 2 hours beyond due date: **10% penalty** to score obtained
- Later than 2 hours: **30% penalty** to score obtained
- 24 hours beyond the due date: **Submissions will not be entertained after 18 Nov 2021, 2359 HRS**

- "Note that this deadline is actually an extended deadline. By right, you should submit the answers by Sunday, 14 Nov. We, however, have given a few extra days at the beginning of the reading week, in case you need some extra time to work on A2."

**Warning**: You are not allowed to test submit flags from our module's past assignments, regardless of how you obtain them. If you are caught intentionally submitting past flags to a given problem, the maximum marks of the problem will be capped at **35%** of its possible marks. This penalty will apply even if you subsequently manage to submit the correct flag.

# Contact

Please direct any inquiries about the assignment to

1. jaryl.loh@u.nus.edu (Jaryl Loh)
2. ye_guoquan@u.nus.edu (Ye Guoquan)
3. e0407206@u.nus.edu (Chan Jian Hao)

Note that the TAs will **not** be debugging your code, but will only be around to discuss high level ideas. Do allow 3 working days for replies. Discussion on forums are highly encouraged.

# Rules and Guidelines

**PLEASE READ THE FOLLOWING BEFORE BEGINNING**

1. You are required to log in to https://cs2107-ctfd-i.comp.nus.edu.sg:8000/ (accessible only within NUS Network) to submit flags before the given deadline.
2. You are additionally required to upload a zip file to the “Student Submission / A2-supporting-files” folder on LumiNUS before the given deadline. The zip file should be named as StudentID_Name.zip (e.g. A01234567_Alice Tan.zip), and it should contain the following:

- A **write up** documenting the approach you took in solving every problem. This must be in PDF format with the following filename format: **StudentID_Name_WU.pdf** (e.g. A01234567_Alice Tan_WU.pdf)
  Note that grades are not determined by this writeup. However, you should strive to be as **detailed** as possible as if you are writing this for someone who is unfamiliar with CTF, such that they could reproduce your steps. Screenshots may be helpful in showing your steps too. If there are suspicion on plagiarism, your writeup may be analysed and you may need to be interviewed by the teaching team to explain your steps. This writeup also serve as proof of your work in case submission server malfunctions.
- All source codes and scripts, if any, in their respective folder based on the challenge name.
- A correct submitted flag but with no write-up submitted will now only earn **35%** of its possible marks.

3. Do not attack any infrastructure not **explicitly authorised** in this document.
4. Multiple flag submission is permitted on the scoring platform without any penalty, but **no bruteforcing of flag submission** will be tolerated.
5. Hints may be released gradually as the assignment progresses. They will be announced at https://cs2107-ctfd-i.comp.nus.edu.sg:8000/announcements, as well as in the LumiNUS forum/announcements.

6. Work **individually**. Discussion of concepts on the forum is allowed but refrain from posting solutions. The university takes plagiarism very seriously. Any sharing of answers detected will be reported and disciplinary actions will be taken.
7. Students may be randomly selected to satisfactorily explain how they obtain their flags. If you **don't respond to our email** requesting you to have an online meeting and briefly explain how you obtain your flags, even after a reminder sent and a reasonable time duration given, we will give you **zero marks**.
8. The skills taught in this assignment are not to be used on any system you do not own or have express permission to test. This is a **criminal offence** under the Singapore Computer Misuse and Cybersecurity Act.
9. All challenges have a solution. They are guaranteed to be solvable with assistance of the internet and some research.
10. Ask the TAs for assistance only after you have exhausted every other avenue of self-help.
11. Every challenge will contain a flag and will provide the accepted flag format. Please ensure your submissions meet the flag format stated **exactly**. This means include the `CS2107{}` portion unless otherwise stated.
12. The challenges are tested from the NUS Wi-Fi within the School of Computing and outside of NUS. Connectivity cannot be guaranteed anywhere else. SoC VPN is **required** if you are outside of school network.

One of the most important skills in the information security field is the skill of seeking an answer independently. It is expected that the participant be able to utilise resources discovered through Google or any other search engine to achieve the tasks.

While the challenges might not be covered in entirety in class, the topics in the assignment are very applicable to security problems in real life. In the long run, the practical skills gained would benefit participants immensely.

# Academic Honesty

NUS students are expected to maintain and uphold the highest standards of integrity and honesty at all times. As this is an **individual assignment**, please refrain from any forms of academic dishonesty.

If any form of plagiarism or cheating is found, you will be penalized and be subject to disciplinary action by the University. You may read more about NUS Student Code of Conduct here.

# Linux Environment (As in Assignment 1)

A Linux system is crucial for solving some of the challenges, the challenges in this section will prepare you for the more advanced sections by presenting some elementary tasks to solve. It is expected that the participant has rudimentary proficiency in using a Linux system that can be gleaned by reading the tutorial at this link: https://www.digitalocean.com/community/tutorials/an-introduction-to-the-linux-terminal.

However, more knowledge might be needed, and it is expected that the participant do some self-exploration.

Do note that you should use a 32-bit / 64-bit Linux environment to aid you in completing some of the challenges. Please also take note that if you are running 64-bit Linux, you may need to run the following commands in Linux to run 32-bit binary executables:

```
sudo dpkg --add-architecture i386
sudo apt-get update
sudo apt-get install -y libc6:i386
```

# Section A: Warmup

The challenges here are to give you a feel of CTF challenges.

## A.1 Grep Food Delivery (2 Points)

I am trying to make an order for a flag, but the menu is a mess! Can you help me find it?

## A.2 Observer (6 Points)

What nefarious thing could be behind this website?
Connect to http://cs2107-ctfd-i.comp.nus.edu.sg:4000/

# Section B: Network

## B.1 Babyshark (3 Points)

To complete this task, please install Wireshark on your Ubuntu or Windows machine.

This can be done via sudo apt-get install wireshark in Ubuntu or manually via: https://www.wireshark.org/download.html

After you have done this. Watch the video at https://www.youtube.com/watch?v=TkCSr30UojM for basic usage of Wireshark

When you are done, inspect the pcap file and find the flag.

## B.2 Mamashark (7 Points)

Mamashark is communicating with the server... but there seems to be cookie authentication??

http://cs2107-ctfd-i.comp.nus.edu.sg:4001

# Section C: Web

*Note: Ensure you are using **HTTP** when visiting the challenges, as HTTPS might cause errors.*

## C.1 Secret Games (18 Points)

We heard there are some fun games going on, perhaps there may be some prize at the end.

Connect to http://cs2107-ctfd-i.comp.nus.edu.sg:4002

## C.2 Bad Client Site (12 Points)

Client site, client side, what could be its down side?

Connect to http://cs2107-ctfd-i.comp.nus.edu.sg:4003

## C.3 Secure Home (12 Points)

I have a file `flag.php` that hackers cannot read.

Oh, and I made a new feature on my website, check it out using URL parameter `f`.

Connect to http://cs2107-ctfd-i.comp.nus.edu.sg:4004/

## C.4 Favourite Tools (18 Points)

I made this site with convenient access to my favorite tools. Give them a try maybe?

Connect to http://cs2107-ctfd-i.comp.nus.edu.sg:4005/

# Section D: Binary

## D.1 BofSchool (7 Points)

Welcome to BofSchool. More instructions are given in the challenge files.

`nc cs2107-ctfd-i.comp.nus.edu.sg 4006`

## D.2 Sneak peek (20 Points)

A cow wants to give you a sneak peek of the flag!
Please be nice and be friendly :)

`ssh sneakpeek@cs2107-ctfd-i.comp.nus.edu.sg -p 12345`

username: sneakpeek
password: sneakpeek

## D.3 Address Book (20 Points)

Address Book is back. CS students love it.

`nc cs2107-ctfd-i.comp.nus.edu.sg 4007`

## D.4 Vegas (25 Points)

Welcome to Las Vegas, the bustling city of lights.
If you are lucky enough, you might strike millions.
Security here is tight, better not get caught!

`nc cs2107-ctfd-i.comp.nus.edu.sg 4008`

Note: no brute force is required to solve this challenge.

# Section F: Bonus

The challenges in this section are out of module scope. They are optional and for additional learning.

## F.1 PWNing Address Book (5 Points)

I have buried another flag in the address book, could you get it?

`nc cs2107-ctfd-i.comp.nus.edu.sg 4007`

Note: The challenge context is the same as the Address Book challenge, but goes deeper. Please solve D.3 before attempting this challenge.

## F.2 Vegas 4fun (5 Points)

Welcome back to Las Vegas!
We have hired a more friendly security team this time. Just enjoy and have fun!

`nc cs2107-ctfd-i.comp.nus.edu.sg 4009`

# Conclusion

We hope you enjoyed the assignment and have learnt something new. Again, please make sure that your flags are correct and contain the flag format **EXACTLY** as stated. This includes the `cs2107{}` tags.

If you found this interesting and would like to play with harder and more interesting CTF problems, please do feel free to contact us at NUS Greyhats.

Best regards,
CS2107 Assignment Team