

# Jason Ngo

Computer Science Major @ UBC

+1 587-890-5411 | work@jasonn.dev | github.com/Green-Avocado

## Skills Summary

<b>Application Security</b>	Buffer overflow, Format-string exploits, Return-oriented programming, Use-after-free
<b>Web Security</b>	SQL injection, Cross-site scripting, Template injection, Local file inclusion, Prototype pollution
<b>Binary Analysis</b>	Ghidra, Radare2, Binary Ninja, GDB, angr, Triton

## Work Experience

2022/05 - 2022/08	<b>Undergraduate Academic Assistant</b> <i>University of British Columbia</i> <ul style="list-style-type: none"> <li>Discovered and patched vulnerabilities in services involving arbitrary code execution and XML injection.</li> <li>Used Python to automate student evaluation on a variety of topics using randomized questions.</li> </ul>
2020/04 - 2022/02	<b>Freelance Software Development</b> <i>Commissioned by clients for various projects. Some examples include:</i> <ul style="list-style-type: none"> <li><u>Transactions database</u> — Designed proof-of-concepts for database solutions using Firebase Realtime Database, MySQL, and Google Drive APIs.</li> <li><u>Mosque timetable</u> — Developed a web application to read data from a CSV file and display prayer times using HTML, CSS, and JavaScript.</li> <li><u>covidping.com</u> — Wrote scripts to load current COVID-19 statistics into Google Sheets and send emails to a list of subscribers for notifying users of COVID-19 statistics in their state.</li> </ul>

## Extracurriculars

2019/09 - Present	<b>Capture The Flag Competitions</b> <a href="https://github.com/Green-Avocado/CTF">https://github.com/Green-Avocado/CTF</a> <ul style="list-style-type: none"> <li>Reverse engineered binaries using static and dynamic analysis techniques.</li> <li>Identified vulnerabilities in binary applications and web services.</li> <li>Defeated common exploit mitigations such as PIE, ASLR, canaries, and RELRO.</li> <li>Created writeups to explain vulnerabilities and exploit techniques used in each challenge.</li> </ul>
-------------------	---

## Projects

2022/05 - 2022/07	<b>No Flag 4 U</b> <a href="https://github.com/Green-Avocado/No-Flag-4-U">https://github.com/Green-Avocado/No-Flag-4-U</a> <ul style="list-style-type: none"> <li>Created a dynamic shared library using Rust to hook standard library functions.</li> <li>Mitigates common vulnerabilities including buffer overflow, format string, and use-after-free.</li> <li>Logs function calls by sending data to an external process using a TCP stream.</li> </ul>
2021/03 - 2022/04	<b>pwndocker</b> <a href="https://github.com/Green-Avocado/pwndocker">https://github.com/Green-Avocado/pwndocker</a> <ul style="list-style-type: none"> <li>Wrote a minimal program in C to create symbolic links without standard libraries.</li> <li>Used Docker to create an environment for debugging exploits under different versions of Glibc.</li> <li>The project became a go-to tool for CTF challenges involving binary exploitation.</li> </ul>
2022/02	<b>BBY Stealer Malware Analysis</b> <a href="https://github.com/Green-Avocado/bbystealer-malware-analysis">https://github.com/Green-Avocado/bbystealer-malware-analysis</a> <ul style="list-style-type: none"> <li>Used Wireshark and Windows filesystem auditing to identify connections and filesystem access.</li> <li>Reverse engineered JavaScript code that was obfuscated and packaged as a Windows executable.</li> <li>Helped victims with incident response by identifying compromised credentials and modified files.</li> </ul>
2021/09 - 2021/12	<b>EasyROP</b> <a href="https://github.com/Green-Avocado/EasyROP">https://github.com/Green-Avocado/EasyROP</a> <ul style="list-style-type: none"> <li>Wrote a Java program using object-oriented design to automate writing scripts for binary exploitation.</li> <li>The project began as a command-line application and later included a GUI using Java Swing.</li> <li>Return-oriented programming payloads could be saved as a local JSON file and reloaded.</li> </ul>

## Education

2020/09 - 2024/04	<b>Bachelor of Science, Major in Computer Science</b> <i>University of British Columbia</i>
2022/04	<b>Program Analysis for Vulnerability Research</b> <i>Vector35 &amp; Margin Research</i>