T: 604.822.9677 | F: 604.822.9677 | science.coop@ubc.ca | www.sciencecoop.ubc.ca

Jason Ngo

Computer Science Major @ UBC

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

Skills Summary

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

Work Experience

2022/05 - 2022/08 **Undergraduate Academic Assistant**
University of British Columbia

- Discovered and patched vulnerabilities in services involving arbitrary code execution and XML injection.
- Used Python to automate student evaluation on a variety of topics using randomized questions.

2020/04 - 2022/02 **Freelance Software Development**
Commissioned by clients for various projects. Some examples include:

- Transactions database — Designed proof-of-concepts for database solutions using Firebase Realtime Database, MySQL, and Google Drive APIs.
- Mosque timetable — Developed a web application to read data from a CSV file and display prayer times using HTML, CSS, and JavaScript.
- covidping.com — 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.

Extracurriculars

2019/09 - Present **Capture The Flag Competitions**
https://github.com/Green-Avocado/CTF

- Reverse engineered binaries using static and dynamic analysis techniques.
- Identified vulnerabilities in binary applications and web services.
- Defeated common exploit mitigations such as PIE, ASLR, canaries, and RELRO.
- Created writeups to explain vulnerabilities and exploit techniques used in each challenge.

Projects

2022/05 - 2022/07 **No Flag 4 U**
https://github.com/Green-Avocado/No-Flag-4-U

- Created a dynamic shared library using Rust to hooks standard library functions.
- Mitigates common vulnerabilities including buffer overflow, format string, and use-after-free.
- Logs function calls by sending data to an external process using a TCP stream.

2021/03 - 2022/04 **pwndocker**
https://github.com/Green-Avocado/pwndocker

- Wrote a minimal program in C to create symbolic links without standard libraries.
- Used Docker to create an environment for debugging exploits under different versions of Glibc.
- The project became a go-to tool for CTF challenges involving binary exploitation.

2022/02 **BBY Stealer Malware Analysis**
https://github.com/Green-Avocado/bbystealer-malware-analysis

- Used Wireshark and Windows filesystem auditing to identify connections and filesystem access.
- Reverse engineered JavaScript code that was obfuscated and packaged as a Windows executable.
- Helped victims with incident response by identifying compromised credentials and modified files.

2021/09 - 2021/12 **EasyROP**
https://github.com/Green-Avocado/EasyROP

- Wrote a Java program using object-oriented design to automate writing scripts for binary exploitation.
- The project began as a command-line application and later included a GUI using Java Swing.
- Return-oriented programming payloads could be saved as a local JSON file and reloaded.

Education

2020/09 - 2024/04 **Bachelor of Science, Major in Computer Science**
University of British Columbia

2022/04 **Program Analysis for Vulnerability Research**
Vector35 & Margin Research