NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

School of Computer Science and Engineering
College of Engineering

Capture-the-Flag Challenges

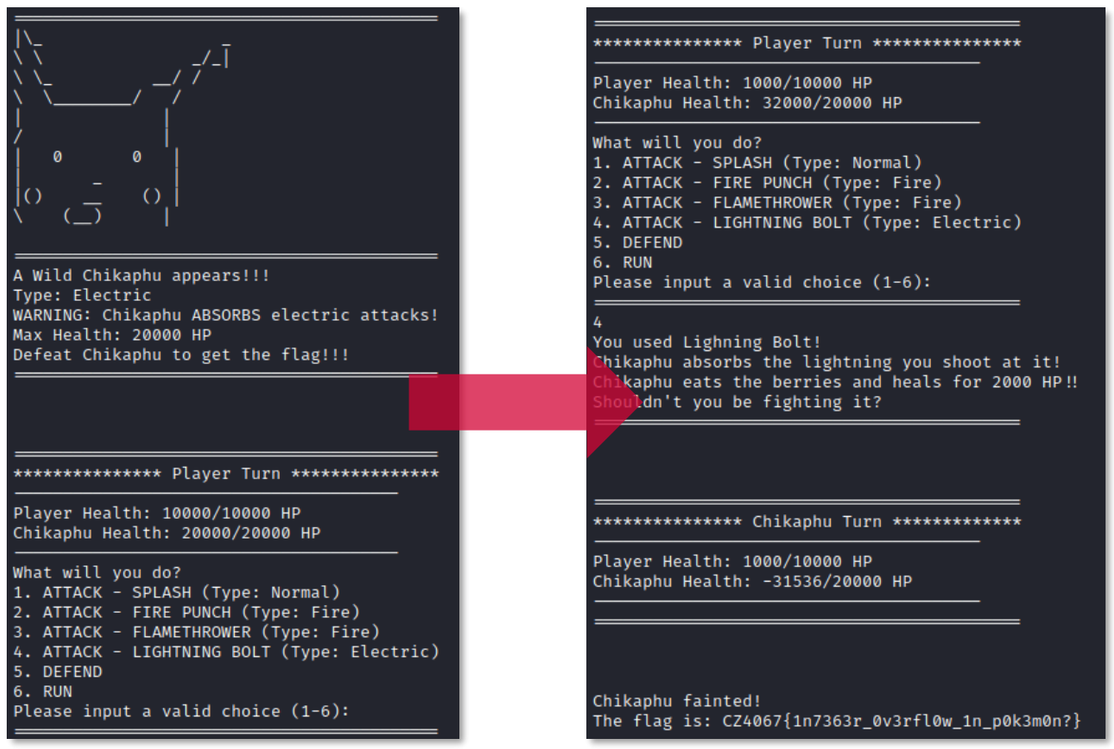
Enhancing cybersecurity education with gamified exercises

Student: Er Jun Jia Supervisor: Assistant Professor Yi Li

Project Objectives:

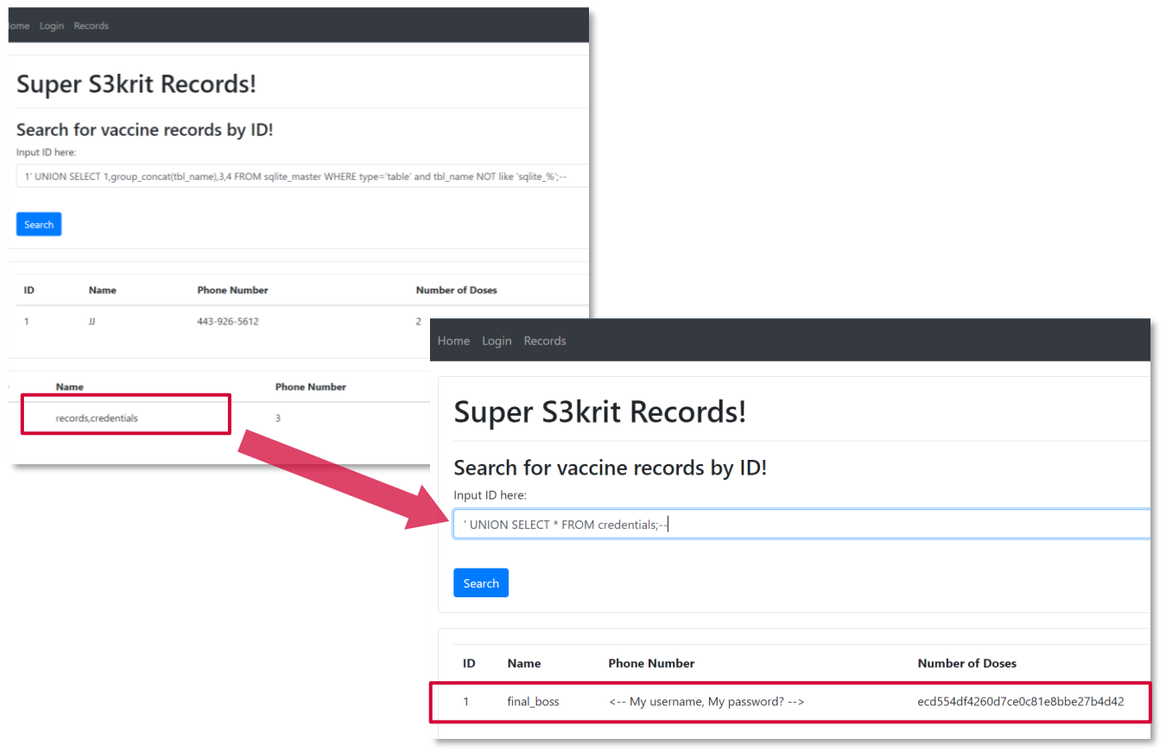
Academic institutions worldwide have harnessed **Capture the Flag (CTF)** cybersecurity challenges as effective educational tools to improve students' cybersecurity skills, knowledge, and experience. To further supplement NTU's CZ4067 Software Security course curriculum and provide a more enriching learning experience for students, this project focuses on the creation and development of relevant and interesting CTF challenges, which will serve as educational tutorial exercises. A total of 14 CTF challenges of varying difficulty were created, with a strong focus on two fundamental cybersecurity categories: Binary Exploitation and Web Hacking.

Binary Exploitation



Binary exploitation attacks bypass intended functionalities of a program. Common exploits include buffer and integer overflows. The screenshots above show an integer overflow challenge in the format of a turn-based *Pokémon* inspired game. By overflowing the maximum HP of the enemy, students can complete the challenge and obtain the flag.

Web Hacking



Web hacking are exploits on web clients, servers and applications. SQL Injection is one of the most popular web attacks, where attackers use client input to read, modify and manipulate SQL databases. The challenge screenshots above show an example of a UNION SELECT SQL Injection attack to maliciously reveal the passwords of the web administrator from a hidden SQL table.