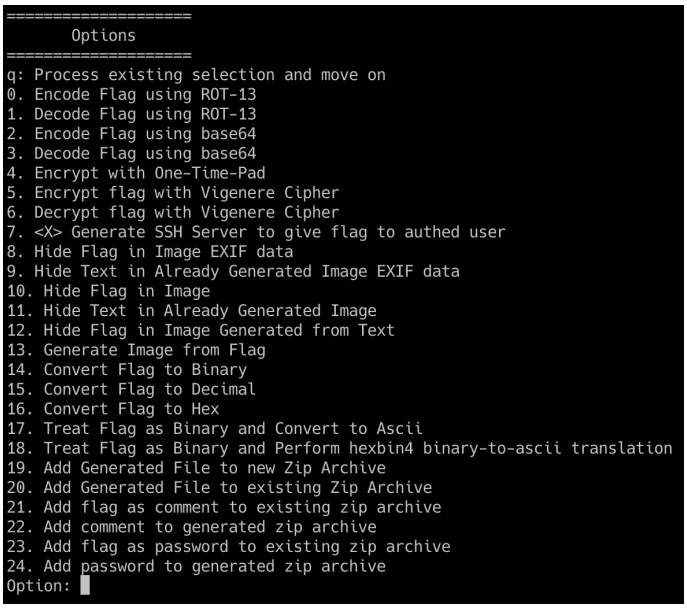
Capture the Flag Challenge Creator



The Terminal UI of the Project

Features

- Module-based tool
- Easy to make new modules
- Easy-to-use interface
- Fully documented schema for modules
- Comes with a variety of modules
- Can be used to create intricate CTF questions
- Creates challenges of all levels of difficulty

Top 3 Issues Faced during Production:

- Found it difficult to make a dynamic module loading system - had to rely on basic sanitization and an 'exec' statement
- Vigenere Cipher doesn't work properly – created a reversible form of encryption which uses a key for encryption and decryption, but doesn't produce standardized output
- Was unable to use the Python Pillow library to achieve steganography – was forced to rely upon *stepic* – a wrapper around Pillow which achieves the same outcome

Report

A four-page report was also constructed detailing the history of Capture the Flag events, and also gives some history and examples of the most frequently asked types of questions involving cryptography, reverse engineers, cross-site scripting and SQL injection.

Capture The Flag

A Capture The Flag event was run from 7th April to the 14th of April. Unfortunately, there were no students able to complete the challenge. Five students were shown a solution to the supplied challenge, and their overall response was that the challenge was deemed too sophisticated for beginners in cybersecurity. However, they all agreed that the challenge was "cool" and agreed that it was innovative how it combined cryptography and forensics.
Link: http://z5214348.web.cse.unsw.edu.au/ctf/