

Capture the Flag Challenge Creator

```
=====
Options
=====
q: Process existing selection and move on
0. Encode Flag using ROT-13
1. Decode Flag using ROT-13
2. Encode Flag using base64
3. Decode Flag using base64
4. Encrypt with One-Time-Pad
5. Encrypt flag with Vigenere Cipher
6. Decrypt flag with Vigenere Cipher
7. <X> Generate SSH Server to give flag to authed user
8. Hide Flag in Image EXIF data
9. Hide Text in Already Generated Image EXIF data
10. Hide Flag in Image
11. Hide Text in Already Generated Image
12. Hide Flag in Image Generated from Text
13. Generate Image from Flag
14. Convert Flag to Binary
15. Convert Flag to Decimal
16. Convert Flag to Hex
17. Treat Flag as Binary and Convert to Ascii
18. Treat Flag as Binary and Perform hexbin4 binary-to-ascii translation
19. Add Generated File to new Zip Archive
20. Add Generated File to existing Zip Archive
21. Add flag as comment to existing zip archive
22. Add comment to generated zip archive
23. Add flag as password to existing zip archive
24. Add password to generated zip archive
Option: 
```

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/>