These writeups, authored by Peyton Braun, are designed to guide you through the process of solving all the challenges from the Inaugural University of Wisconsin – Stout Cybersecurity Capture the Flag (CTF) event.

This event was hosted by UW-Stout CyROC x CCDL

I hope these writeups help you gain a deeper understanding of each challenge and how to overcome them.

CTF Challenge Writeups

Each writeup will cover the following aspects of the challenge:

1. **Challenge Overview**: A brief description of the challenge.
2. **Steps to Solve**: Detailed steps, tools used, and reasoning behind each step.
3. **Tools and Methods**: Explanation of why specific tools and methods were chosen.
4. **How It Works**: Insight into the underlying concepts and the thinking process.

Challenge: "Who said 30 times?"

Challenge Overview:

Decode a hexdump file containing a flag encoded with base64 30 times.

Challenge Description:

- What strange encoding. Can you decipher it to get the flag?

Steps to Solve:

1. Extract the information from the hexdump file:
    - Use CyberChef's "From Hexdump" operation to convert the hexdump into a readable format.
2. Decode the base64 string 30 times:
    - Use CyberChef's "From Base64" operation in a loop or a custom script.
3. Retrieved flag:
    - STOUTCTF{djfRQP4yBWjbcnEEixBHvUvta8iZd5Fm}.

Tools and Methods:

- **CyberChef**: Simplifies repeated decoding operations.
- **Custom Script**: Useful for automating repetitive tasks (e.g., using Python).

How It Works:

Hexdump represents binary data in hexadecimal format. Base64 decoding multiple times involves reversing the encoding process repeatedly.