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: "Based"

Challenge Overview:

Decode a base64 string to retrieve the flag.

Challenge Description:

- This challenge is Based

Steps to Solve:

1. Obtain the base64 string provided in the challenge description:
    - U1RPVVRDVEZ7aFM1RFRKYzEyYkR5N3NxSm9lN3FRczdkWHJFNFlzZDd9.
2. Use a decoding tool such as CyberChef.
    - Select the "From Base64" operation.
    - Paste the encoded string into the input field.
3. Execute the operation to reveal the decoded flag.
4. Retrieved flag:
    - STOUTCTF{hS5DTJc12bDy7sqJoH7qQs7dXrE4Ysd7}.

Tools and Methods:

- **CyberChef**: Chosen for its simplicity and wide range of encoding/decoding capabilities.

How It Works:

Base64 is an encoding scheme that represents binary data in an ASCII string format. Decoding it reverses this process to reveal the original data. CyberChef’s "From Base64" operation automatically handles this.