

**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: "Nothing To See Here!"**

#### **Challenge Overview:**

This challenge involves extracting hidden information encoded in whitespace within a seemingly empty file. The solution requires multiple decoding steps, including interpreting the whitespace, Base64 decoding, gzip decompression, and a secondary whitespace decoding to reveal the flag.

#### **Challenge Description:**

- Seriously, what are you looking at?

#### **Challenge Hints:**

- What do they call the empty space between or around objects? I think that might be useful here, and its not negative, think in a document. Maybe color, or the lack of color, depends on how you see it.
- Sanity hint, there is no hex involved in this challenge ;)

#### **Steps to Solve:**

1. **Load Whitespace Code into Interpreter:**
  1. Input the contents of the provided file into the whitespace interpreter on [dcode.fr](https://dcode.fr) to extract the encoded message.
2. **Decode Base64:**
  1. Take the output from the whitespace interpreter and decode it using CyberChef with the "From Base64" operation.

### 3. Check for Compression:

1. Analyze the entropy of the decoded Base64 result. Discover that the content is gzip-compressed.

### 4. Decompress Gzip:

1. Use CyberChef's "GUNZIP" operation to decompress the data. This step reveals the text "**Nothing to see here!**" with another set of whitespace code underneath.

### 5. Repeat Whitespace Decoding:

1. Copy the second layer of whitespace code and input it back into the whitespace interpreter.

### 6. Extract the Flag:

1. The output from the second whitespace decoding reveals the flag.

### 7. Decoded Flag:

1. STOUTCTF{ab6lcT8R4vNyAJNWQteBJ3Yd2VTrkVCp}

## Tools and Methods:

- **Tools Used:**

- <https://www.dcode.fr/whitespace-language>
- CyberChef

- **Methodology:** A stepwise decoding process leveraging encoding/decoding knowledge and specialized tools.

## How It Works:

The challenge demonstrates multi-layered encoding by hiding information in whitespace, then further encoding it through Base64 and gzip compression. Each step requires logical thinking and familiarity with data encoding formats.