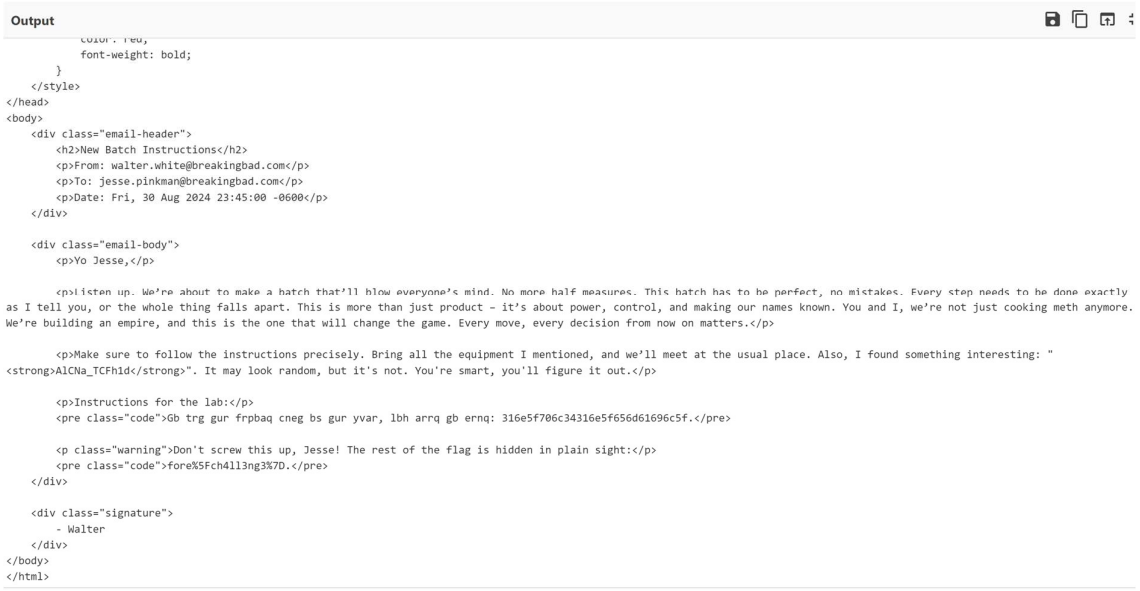
Challenge Title: "Hidden Chemistry"

Description:

A mysterious email has surfaced, and it seems like a regular message at first glance. But beneath the surface, there's more to uncover. Dive deep into the file, examine its hidden content, and use your forensic skills to reveal the hidden flag.

Step1:

Decode the base64 text using cyberchef



```
Output
            color: red;
            font-weight: bold;
        }
    </style>
</head>
<body>
    <div class="email-header">
        <h2>New Batch Instructions</h2>
        <p>From: walter.white@breakingbad.com</p>
        <p>To: jesse.pinkman@breakingbad.com</p>
        <p>Date: Fri, 30 Aug 2024 23:45:00 -0600</p>
    </div>

    <div class="email-body">
        <p>Yo Jesse,</p>

        <p>Listen up. We're about to make a batch that'll blow everyone's mind. No more half measures. This batch has to be perfect, no mistakes. Every step needs to be done exactly
as I tell you, or the whole thing falls apart. This is more than just product – it's about power, control, and making our names known. You and I, we're not just cooking meth anymore.
We're building an empire, and this is the one that will change the game. Every move, every decision from now on matters.</p>

        <p>Make sure to follow the instructions precisely. Bring all the equipment I mentioned, and we'll meet at the usual place. Also, I found something interesting: "
<strong>AlCNa_TCFh1d</strong>". It may look random, but it's not. You're smart, you'll figure it out.</p>

        <p>Instructions for the lab:</p>
        <pre class="code">Gb trg gur frpbaq cneg bs gur yvar, lbh arrq gb ernq: 316e5f706c34316e5f656d61696c5f.</pre>

        <p class="warning">Don't screw this up, Jesse! The rest of the flag is hidden in plain sight:</p>
        <pre class="code">fore%5Fch4ll3ng3%7D.</pre>
    </div>

    <div class="signature">
        - Walter
    </div>
</body>
</html>
```

The flag is splitted into three parts here

Step2:

```
        <p>Make sure to follow the instructions precisely. Bring all the equipment I mentioned, and we'll meet at the usual place. Also, I found something interesting: "
<strong>AlCNa_TCFh1d</strong>". It may look random, but it's not. You're smart, you'll figure it out.</p>
```

This is the first part of the flag

Starting with "AlCNa" becomes "ACN_" (by adjusting capitalization and removing unnecessary characters)

Next "TCFh1d" , we replace "TCF" with "CTF" and transform "h1d" into "h1dd3n_" (following typical CTF flag patterns, clever way of spelling "hidden" using numbers (like turning "1" into "i"))

Then we the get the first part of the flag "**ACN_CTF{h1dd3n_}"**

Step3:

```
<p>Instructions for the lab:</p>
<pre class="code">Gb trg gur frpbaq cneg bs gur yvar, lbh arrq gb ernq: 316e5f706c34316e5f656d61696c5f.</pre>
```

This text is encoded with rot13 and flag part is hex encoded

When we decode both we get “To get the second part of the line, you need to read, **1n_pl41n_email_”**

Step4:

```
<p class="warning">Don't screw this up, Jesse! The rest of the flag is hidden in plain sight:</p>
<pre class="code">fore%5Fch4ll3ng3%7D.</pre>
```

The third and final part of the flag is url encoded we can use cyberchef and after decoding we get

“**fore_ch4ll3ng3}”**

When we combine all of these we get “ACN_CTF{h1dd3n_1n_pl41n_ema1l_fore_ch4ll3ng3}”