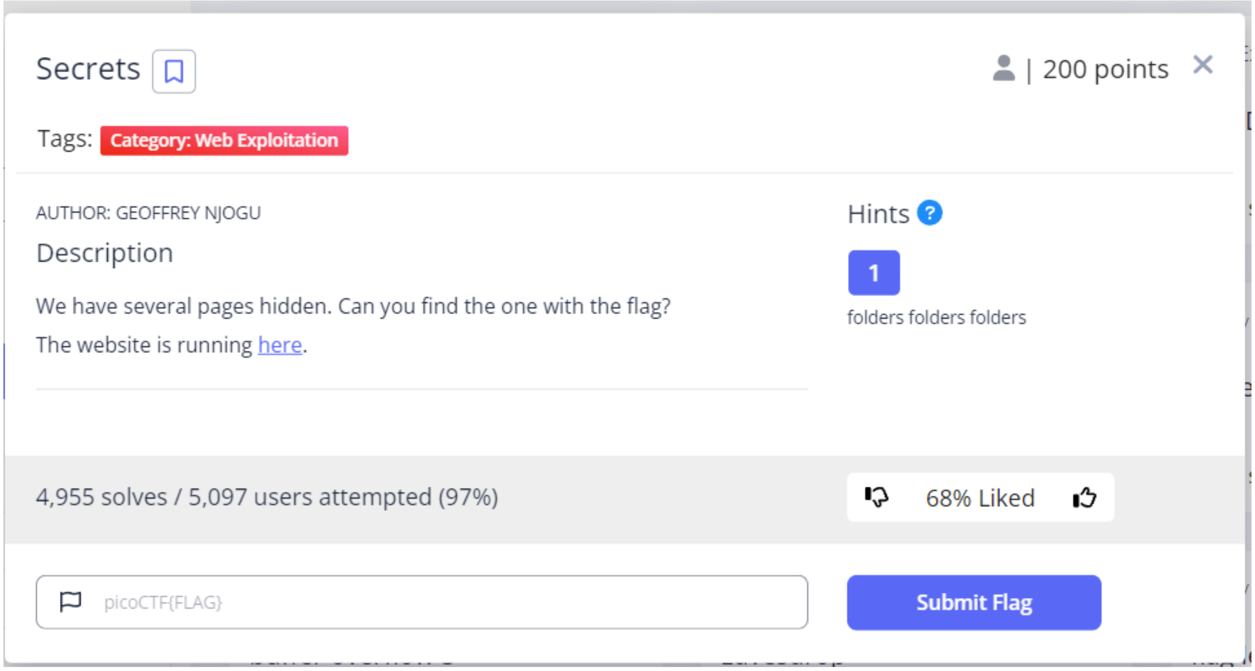
PicoCTF 2022 #38 ‘Secrets’ HIDDEN WEBSITE DIRECTORIES



Secrets

Tags: Category: Web Exploitation

AUTHOR: GEOFFREY NJOGU

Description

We have several pages hidden. Can you find the one with the flag?

The website is running here.

Hints

1

folders folders folders

4,955 solves / 5,097 users attempted (97%)

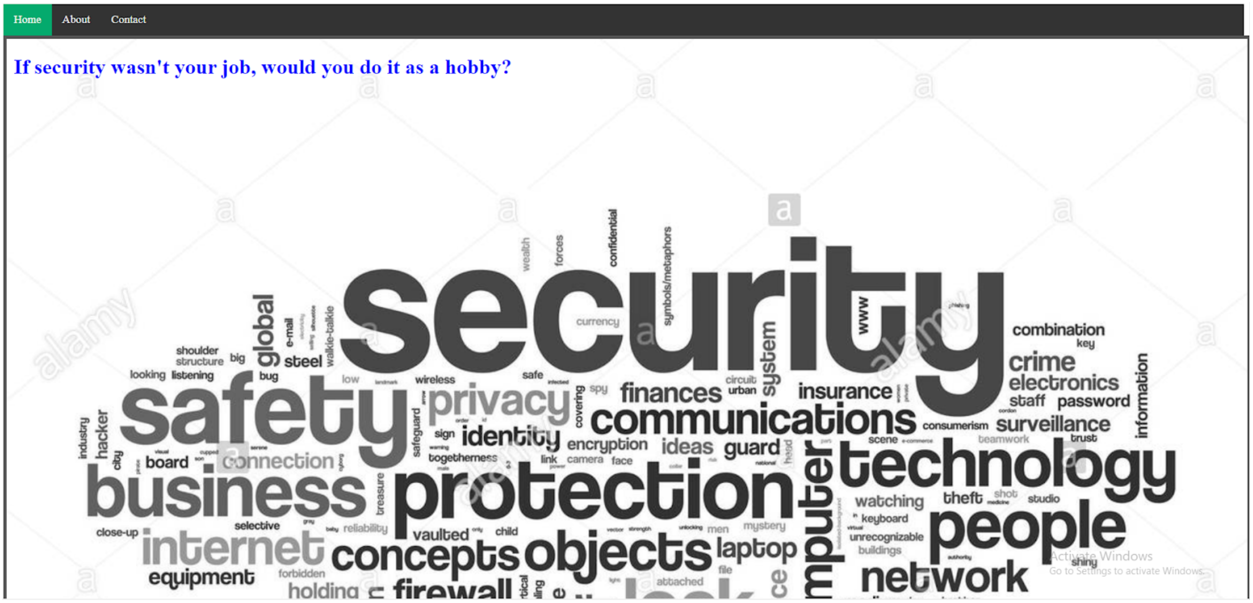
What is a Website Directory?

A website directory is a handmade list of websites. Also known as a subject directory, these lists create an organized method for finding websites. It's similar, but not identical, to a search engine.

LET'S BEGIN OUR CTF

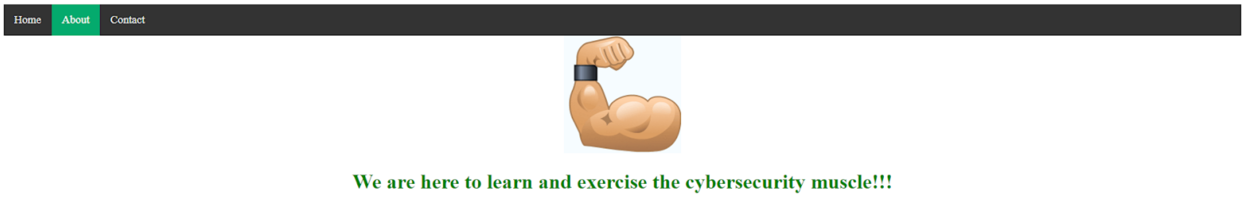
As we begin , we are greeted with three web pages

Page 1 - Home Page



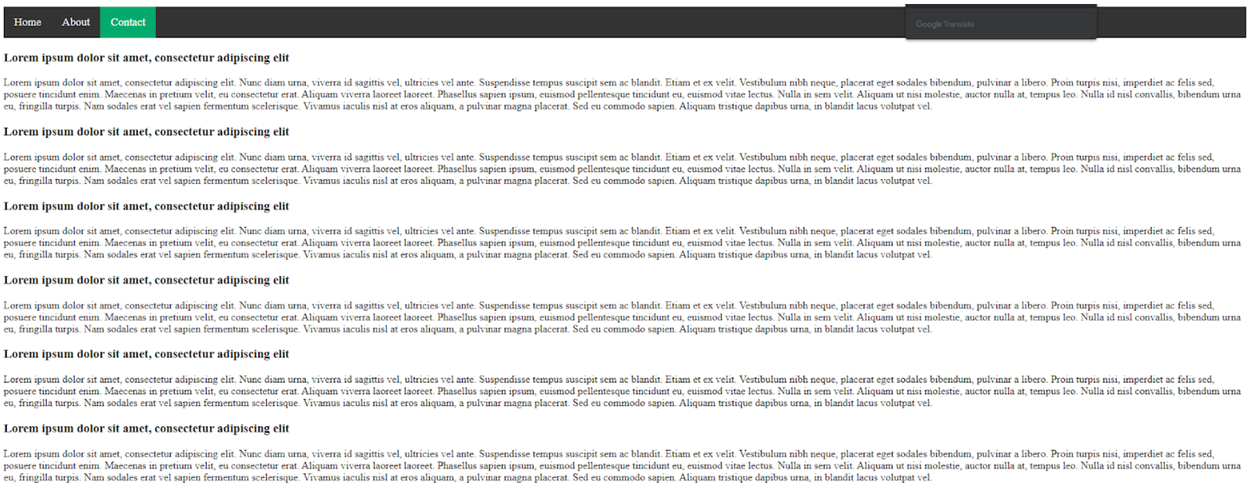
If security wasn't your job, would you do it as a hobby?

Page 2 - About



We are here to learn and exercise the cybersecurity muscle!!!

Page 3 - Contact



Lorem ipsum dolor sit amet, consectetur adipiscing elit

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc diam urna, viverra id sagittis vel, ultricies vel ante. Suspendisse tempus suscipit sem ac blandit. Etiam et ex velit. Vestibulum nibh neque, placerat eget sodales bibendum, pulvinar a libero. Proin turpis nisi, imperdiet ac felis sed, posuere tincidunt enim. Maecenas in pretium velit, eu consectetur erat. Aliquam viverra laoreet laoreet. Phasellus sapien ipsum, euismod pellentesque tincidunt eu, euismod vitae lectus. Nulla in sem velit. Aliquam ut nisi molestie, auctor nulla at, tempus leo. Nulla id nisl convallis, bibendum urna eu, fringilla turpis. Nam sodales erat vel sapien fermentum scelerisque. Vivamus iaculis nisl at eros aliquam, a pulvinar magna placerat. Sed eu commodo sapien. Aliquam tristique dapibus urna, in blandit lacus volutpat vel.

Lorem ipsum dolor sit amet, consectetur adipiscing elit

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc diam urna, viverra id sagittis vel, ultricies vel ante. Suspendisse tempus suscipit sem ac blandit. Etiam et ex velit. Vestibulum nibh neque, placerat eget sodales bibendum, pulvinar a libero. Proin turpis nisi, imperdiet ac felis sed, posuere tincidunt enim. Maecenas in pretium velit, eu consectetur erat. Aliquam viverra laoreet laoreet. Phasellus sapien ipsum, euismod pellentesque tincidunt eu, euismod vitae lectus. Nulla in sem velit. Aliquam ut nisi molestie, auctor nulla at, tempus leo. Nulla id nisl convallis, bibendum urna eu, fringilla turpis. Nam sodales erat vel sapien fermentum scelerisque. Vivamus iaculis nisl at eros aliquam, a pulvinar magna placerat. Sed eu commodo sapien. Aliquam tristique dapibus urna, in blandit lacus volutpat vel.

Lorem ipsum dolor sit amet, consectetur adipiscing elit

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc diam urna, viverra id sagittis vel, ultricies vel ante. Suspendisse tempus suscipit sem ac blandit. Etiam et ex velit. Vestibulum nibh neque, placerat eget sodales bibendum, pulvinar a libero. Proin turpis nisi, imperdiet ac felis sed, posuere tincidunt enim. Maecenas in pretium velit, eu consectetur erat. Aliquam viverra laoreet laoreet. Phasellus sapien ipsum, euismod pellentesque tincidunt eu, euismod vitae lectus. Nulla in sem velit. Aliquam ut nisi molestie, auctor nulla at, tempus leo. Nulla id nisl convallis, bibendum urna eu, fringilla turpis. Nam sodales erat vel sapien fermentum scelerisque. Vivamus iaculis nisl at eros aliquam, a pulvinar magna placerat. Sed eu commodo sapien. Aliquam tristique dapibus urna, in blandit lacus volutpat vel.

Lorem ipsum dolor sit amet, consectetur adipiscing elit

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc diam urna, viverra id sagittis vel, ultricies vel ante. Suspendisse tempus suscipit sem ac blandit. Etiam et ex velit. Vestibulum nibh neque, placerat eget sodales bibendum, pulvinar a libero. Proin turpis nisi, imperdiet ac felis sed, posuere tincidunt enim. Maecenas in pretium velit, eu consectetur erat. Aliquam viverra laoreet laoreet. Phasellus sapien ipsum, euismod pellentesque tincidunt eu, euismod vitae lectus. Nulla in sem velit. Aliquam ut nisi molestie, auctor nulla at, tempus leo. Nulla id nisl convallis, bibendum urna eu, fringilla turpis. Nam sodales erat vel sapien fermentum scelerisque. Vivamus iaculis nisl at eros aliquam, a pulvinar magna placerat. Sed eu commodo sapien. Aliquam tristique dapibus urna, in blandit lacus volutpat vel.

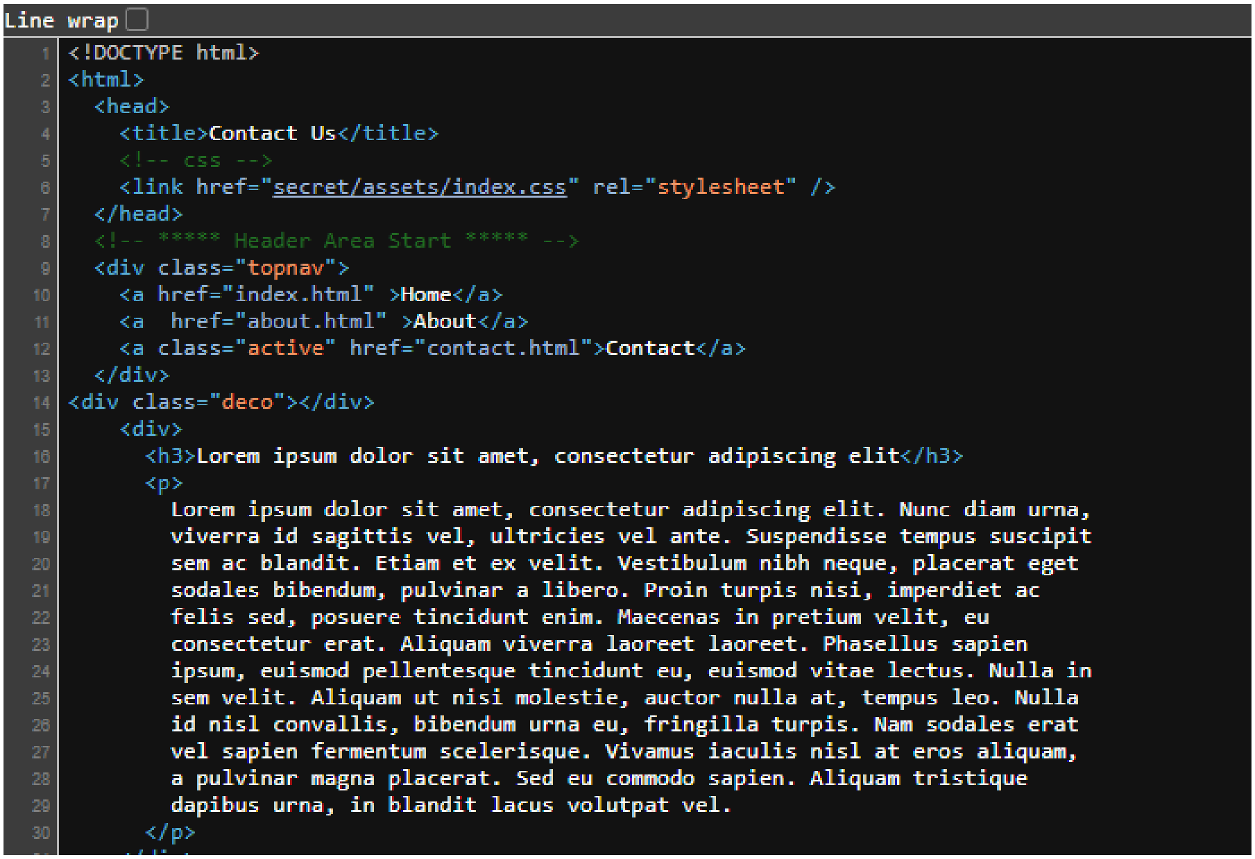
Lorem ipsum dolor sit amet, consectetur adipiscing elit

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc diam urna, viverra id sagittis vel, ultricies vel ante. Suspendisse tempus suscipit sem ac blandit. Etiam et ex velit. Vestibulum nibh neque, placerat eget sodales bibendum, pulvinar a libero. Proin turpis nisi, imperdiet ac felis sed, posuere tincidunt enim. Maecenas in pretium velit, eu consectetur erat. Aliquam viverra laoreet laoreet. Phasellus sapien ipsum, euismod pellentesque tincidunt eu, euismod vitae lectus. Nulla in sem velit. Aliquam ut nisi molestie, auctor nulla at, tempus leo. Nulla id nisl convallis, bibendum urna eu, fringilla turpis. Nam sodales erat vel sapien fermentum scelerisque. Vivamus iaculis nisl at eros aliquam, a pulvinar magna placerat. Sed eu commodo sapien. Aliquam tristique dapibus urna, in blandit lacus volutpat vel.

Lorem ipsum dolor sit amet, consectetur adipiscing elit

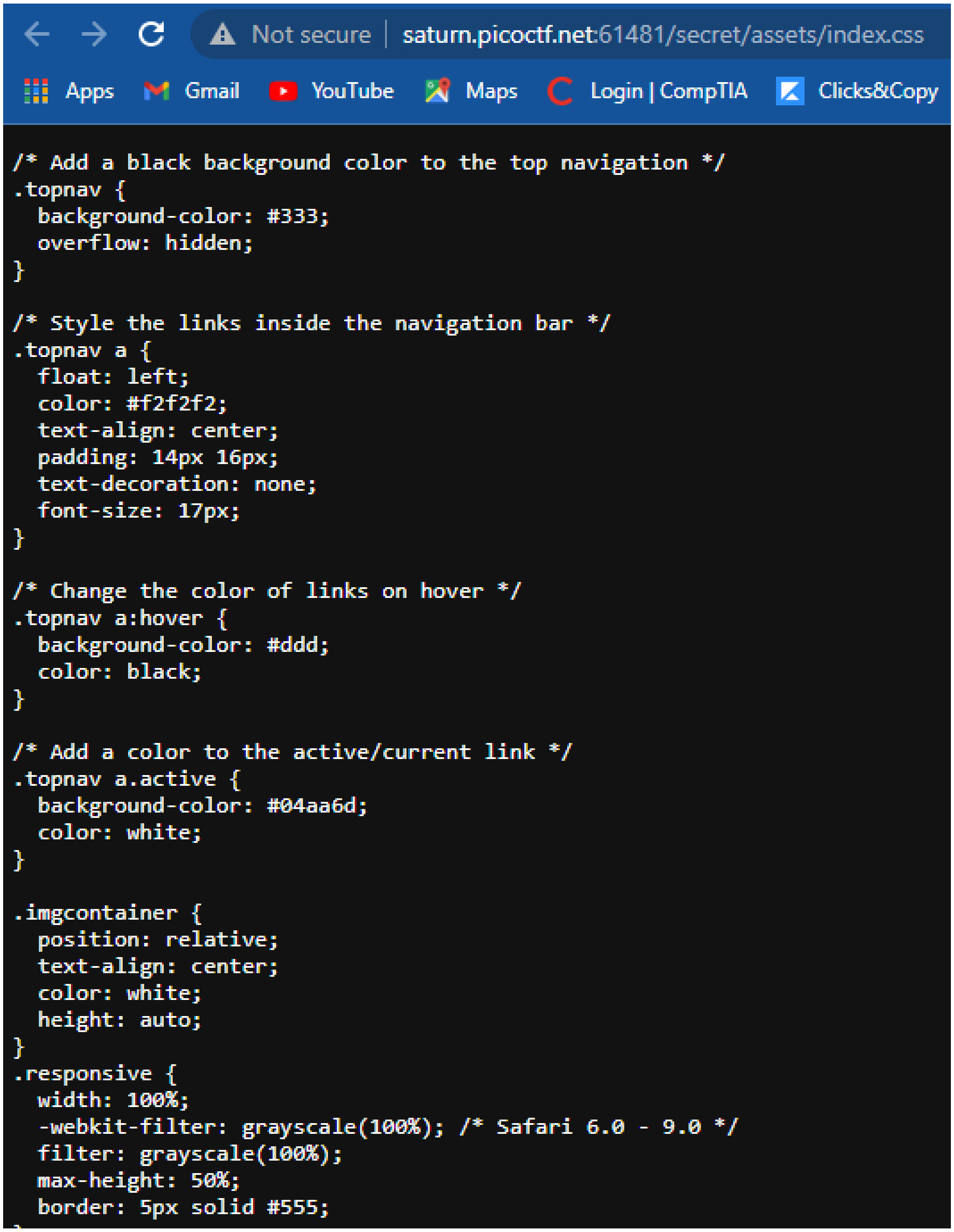
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc diam urna, viverra id sagittis vel, ultricies vel ante. Suspendisse tempus suscipit sem ac blandit. Etiam et ex velit. Vestibulum nibh neque, placerat eget sodales bibendum, pulvinar a libero. Proin turpis nisi, imperdiet ac felis sed, posuere tincidunt enim. Maecenas in pretium velit, eu consectetur erat. Aliquam viverra laoreet laoreet. Phasellus sapien ipsum, euismod pellentesque tincidunt eu, euismod vitae lectus. Nulla in sem velit. Aliquam ut nisi molestie, auctor nulla at, tempus leo. Nulla id nisl convallis, bibendum urna eu, fringilla turpis. Nam sodales erat vel sapien fermentum scelerisque. Vivamus iaculis nisl at eros aliquam, a pulvinar magna placerat. Sed eu commodo sapien. Aliquam tristique dapibus urna, in blandit lacus volutpat vel.

As we see no useful information relating to our CTF challenge , lets go ahead and view the source code using the command “Control + U”



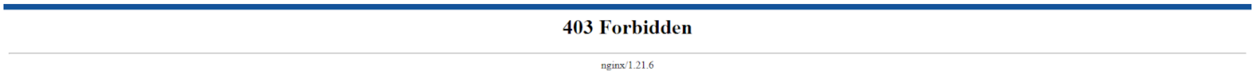
```
<!DOCTYPE html>
<html>
  <head>
    <title>Contact Us</title>
    <!-- css -->
    <link href="secret/assets/index.css" rel="stylesheet" />
  </head>
  <!-- ***** Header Area Start ***** -->
  <div class="topnav">
    <a href="index.html" >Home</a>
    <a  href="about.html" >About</a>
    <a class="active" href="contact.html">Contact</a>
  </div>
<div class="deco"></div>
    <div>
      <h3>Lorem ipsum dolor sit amet, consectetur adipiscing elit</h3>
      <p>
        Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc diam urna,
        viverra id sagittis vel, ultricies vel ante. Suspendisse tempus suscipit
        sem ac blandit. Etiam et ex velit. Vestibulum nibh neque, placerat eget
        sodales bibendum, pulvinar a libero. Proin turpis nisi, imperdiet ac
        felis sed, posuere tincidunt enim. Maecenas in pretium velit, eu
        consectetur erat. Aliquam viverra laoreet laoreet. Phasellus sapien
        ipsum, euismod pellentesque tincidunt eu, euismod vitae lectus. Nulla in
        sem velit. Aliquam ut nisi molestie, auctor nulla at, tempus leo. Nulla
        id nisl convallis, bibendum urna eu, fringilla turpis. Nam sodales erat
        vel sapien fermentum scelerisque. Vivamus iaculis nisl at eros aliquam,
        a pulvinar magna placerat. Sed eu commodo sapien. Aliquam tristique
        dapibus urna, in blandit lacus volutpat vel.
      </p>
```

While studying the source code , we see a link that seems interesting “<link href="secret/assets/index.css" rel="stylesheet" />” and we click it, it takes us to



```
/* Add a black background color to the top navigation */
.topnav {
  background-color: #333;
  overflow: hidden;
}

/* Style the links inside the navigation bar */
.topnav a {
  float: left;
  color: #f2f2f2;
  text-align: center;
  padding: 14px 16px;
  text-decoration: none;
  font-size: 17px;
}

/* Change the color of links on hover */
.topnav a:hover {
  background-color: #ddd;
  color: black;
}

/* Add a color to the active/current link */
.topnav a.active {
  background-color: #04aa6d;
  color: white;
}

.imgcontainer {
  position: relative;
  text-align: center;
  color: white;
  height: auto;
}
.responsive {
  width: 100%;
  -webkit-filter: grayscale(100%); /* Safari 6.0 - 9.0 */
  filter: grayscale(100%);
  max-height: 50%;
  border: 5px solid #555;
```

Still no useful information to be found. But on a second glance we see the url, and try to go back a little before index to assets.



403 Forbidden

nginx/1.21.6

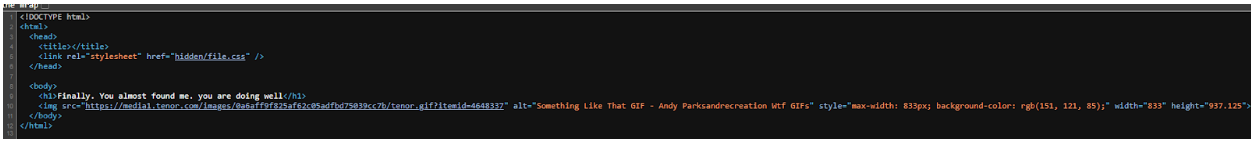
It returns a 403 Forbidden message , so a dead end.

So now we go back a step more in the url to the secrets

http://saturn.picoctf.net:61481/secret/

Finally. You almost found me. you are doing well

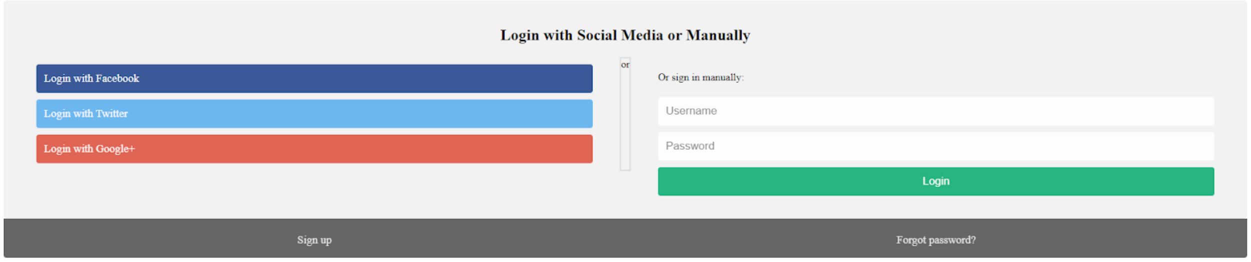
A very comic message greets us , so lets check its souce code



```html
<!DOCTYPE html>
<html>
  <head>
    <title></title>
    <link rel="stylesheet" href="hidden/file.css" />
  </head>

  <body>
    <h1>Finally. You almost found me. you are doing well</h1>
    <img src="https://media1.tenor.com/images/0a6aff9f825af62c05adfbd75039cc7b/tenor.gif?itemid=4648337" alt="Something Like That GIF - Andy Parksandrecreation Wtf GIFs" style="max-width: 833px; background-color: rgb(151, 121, 85);" width="833" height="937.125">
  </body>
</html>
```

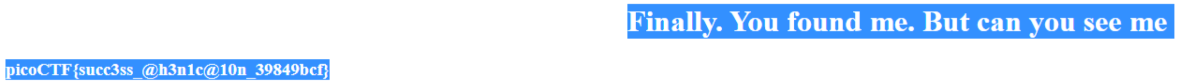
In the source code a we find a link “`<link rel="stylesheet" href="hidden/file.css" /`”

When we go to the link and further investigate we are greeted by this page



We further review the source code of this page and find a very interesting link “`<input type="hidden" name="db" value="superhidden/xdfgwd.html" />`”

We copy and paste the superhidden/ to the page code (http://saturn.picoctf.net:61481/secret/hidden/superhidden/) and press ENTER


Finally. You found me. But can you see me

picoCTF{succ3ss_@h3n1c@10n_39849bcf}

WE DID IT, WE CAPTURED THE FLAG

Thanks For Reading, Have A Good DAY!