picoCTF

Search Source

Isaac Falero

IS 401/501

10/24/2023

Description: The developer of this website mistakenly left an important artifact in the website source, can you find it?

Website: http://saturn.picoctf.net:65086/index.html

Hint: How could you mirror the website on your local machine so you could use more powerful tools for searching?

Upon opening the link, we are directed to a webpage for Flexed Yoga:

1. To begin, we can search in the source code, the index.html file and all its JavaScript and PNG assets, for any clues. However, there's just so much to dig through.
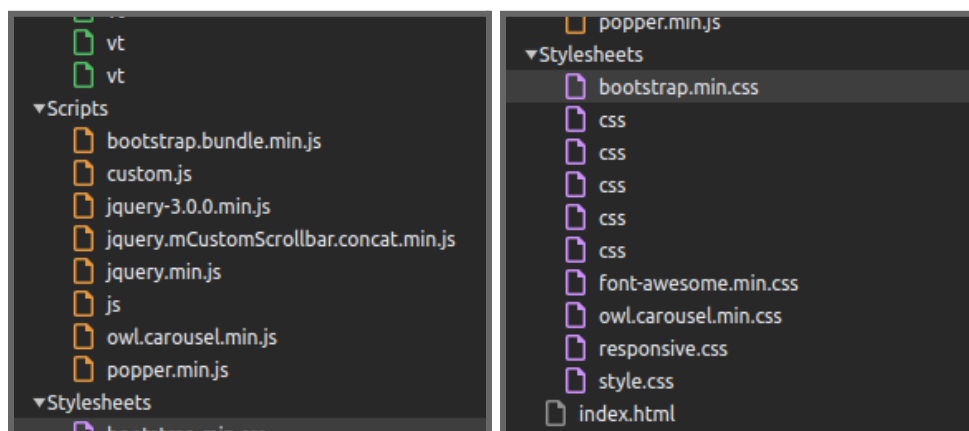
```
            </a>
        </div>
    </div>
    <!-- end slider section -->

    <!-- six_box
    end six_box    The flag is not here but keep digging :)-- >

    <!-- We Do Yogas -->
    <div id="yoga" class="weyoga">
        <div class="container">
            <div class="row">
                <div class="col-md-12">
```

2. Looking to the hint for some direction, it tells us to consider mirroring the website on our local machine to have access to more powerful search tools.

3. To mirror the website on our local machine, we'll use the command "wget -m http://saturn.picoctf.net:65086/index.html" in the terminal. This "-m" flag will mirror the referenced website by creating a directory called "saturn.picoctf.net:65086" with all of the website's assets.

```
:~/picoctf$ wget -m http://saturn.picoctf.net:65086/index.html
-  http://saturn.picoctf.net:65086/index.html
tf.net (saturn.picoctf.net)... 13.59.203.175
icoctf.net (saturn.picoctf.net)|13.59.203.175|:65086... connected.
iting response... 200 OK
```

```
saturn.picoctf.net:65086
```

4. Now, we can use the command "grep -ir picoctf saturn.picoctf.net\:65086/" to find the string "picoctf." The "-i" flag ensures that the search is not case sensitive and the "-r" flag ensures we are recursively searching in all the files and all the subdirectories of the specified directory.

```
:~/picoctf$ grep -ir picoctf saturn.picoctf.net\:65086/
36/css/style.css:/** banner_main picoCTF{1nsp3ti0n_0f_w3bpag3s_587d12b8} **/
```

Flag: picoCTF{1nsp3ti0n_0f_w3bpag3s_587d12b8}