Guilherme Alt Chagas Merklein

PicoCTF 2024 - Web Exploitation

flag: picoCTF{pr3tty_c0d3_d9c45a0b}

26/03/2024

Unminify

This challenge provides you with a webpage (image 1) that tells you your browser has successfully received the flag. First thing I do in these kinds of challenges is open the browser's element inspector and search for the flag or clues in the HTML code. In this specific one, I opened all the divs but there was no flag. All that was were a bunch of components of a class with name "picoctf{}" (image 2). My second thought after inspecting the elements is usually to open svg files imported by the main page or intercept the page's HTTP response with wireshark, but it was not necessary in this one.

Image 1: website's home page.

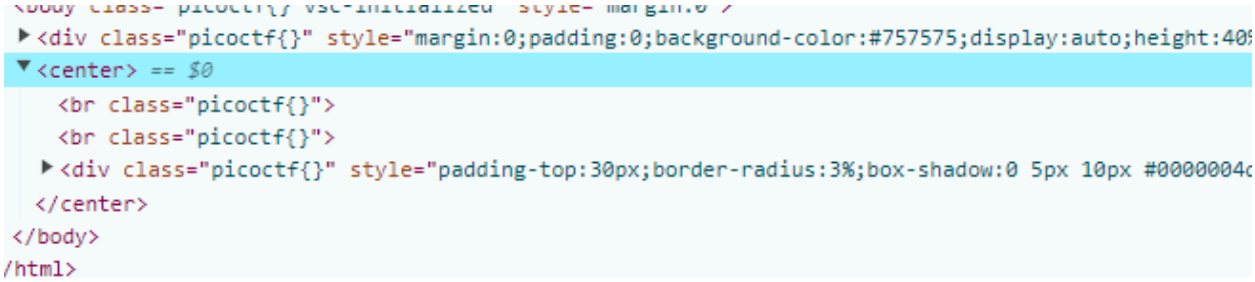

Image 2: Example of html elements with the class “picoctf{}“

After inspecting, I opened the page’s source code (honestly not expecting much), which is a functionality also provided by the browser, and actually got the flag. Honestly, didn’t know why it works like this and I didn’t even stop to research. This task is left as homework for the reader.

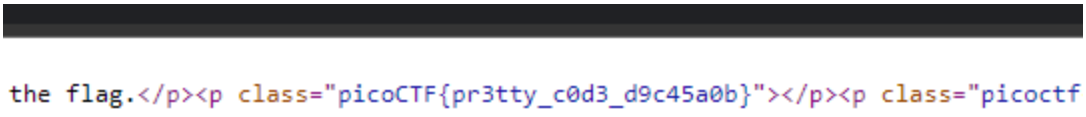

Image 3: Part of the page’s source code.