Guilherme Alt Chagas Merklein

PicoCTF 2024 - Web Exploitation

flag: picoCTF{web_succ3ssfully_d3c0ded_07b91c79}

26/03/2024

WebDecode

Okay, this one kind of pissed me off, and it is entirely my fault. It is supposed to be an easy problem, but I was so blind and kept searching for far more time than I should have.

I was presented with a web page with a very questionable layout, telling me to keep searching for the flag (images 1 and 2). First thing I did was look at the other webpages for any clues (Home, About and Contact). I found nothing at first glance so I did the usual strategy: inspect the elements and search for clues there.

I opened all the divs in the home page, but did not find any flag. Then I went to the contact page and ~~found the base-64 encoded flag after opening some divs~~ and found nothing. Then to the contact page and also nothing.

I thought that I would have to check the files that came together with the website, like the stytles.css, the images and even the custom fonts that were being hosted in another server. Got nothing. I opened wireshark to capture the responses and see if I missed something. I saw nothing, and was starting to lose patience, since it was supposed to be easy.

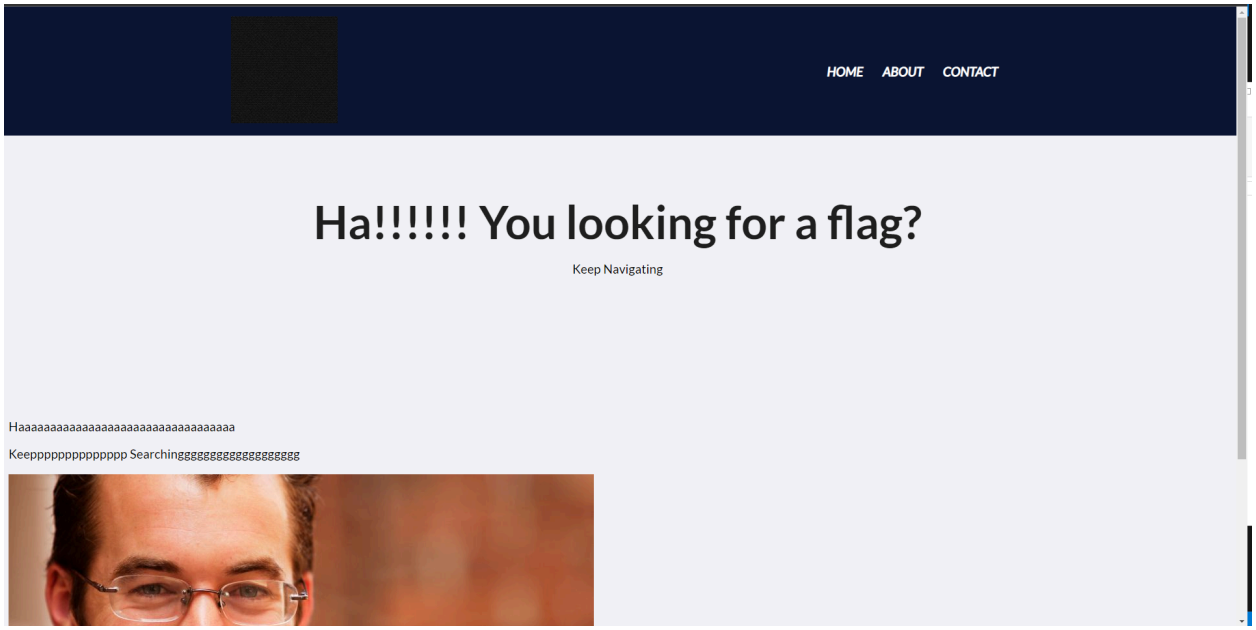

Image 1: home page (top).

Image 2: home page (bottom).

I revisited the pages many times and each time I saw that guy with a smirk on his face on the home page I would lose my patience even more. After searching some more I found a suspicious string on the contact page (image 3). It was just in a div, I should have seen it before but idk.

It 's not over. I thought every base-64 encoded message would have its final characters as being “==”, so my initial thought was not using base64. I tried rot13 and caesar’s cipher, but got nothing.

Image 3: Base64-encoded flag.

After decoding the message with an online decoder, I finally got the flag:

picoCTF{web_succ3ssfully_d3c0ded_07b91c79}