dont-use-client-side

The challenge “dont-use-client-side” was all about trying to get into what was thought to be a secure portal. Once the instance was running, I accessed the browser inspector instead of trying to find the passwords. In the JavaScript code, I found the verify() function that handled the entire process of authentication on the client side.

The code segmented the password into four-character chunks and compared them to pre-set values using substring comparisons. Each line revealed a part of the flag. I wrote down all the chunks and rearranged them based on their positions, creating a string.

This recreated the entire flag: picoCTF{no_clients_plz_2eb02b45}.

The important thing to remember here is that it is very simple. Once the validation is done in JavaScript, it is very easy for anyone to see the code and reverse engineer it. The correct way to validate is on the server side.