dont-use-client-side:

Web Exploitation

Description

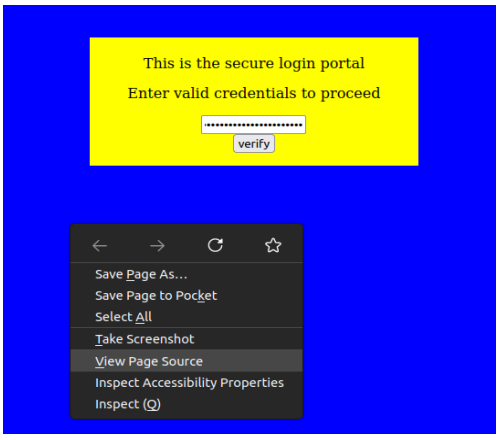
Can you break into this super secure portal?
https://jupiter.challenges.picoctf.org/problem/37821/ (link) or
http://jupiter.challenges.picoctf.org:37821

Hints:

1) Never trust the client

Solution:

1) We look at the page source to find that the flag is right in front of us bus it is divided into parts.




```
 8
 9 <script type="text/javascript">
10   function verify() {
11     checkpass = document.getElementById("pass").value;
12     split = 4;
13     if (checkpass.substring(0, split) == 'pico') {
14       if (checkpass.substring(split*6, split*7) == 'a3c8') {
15         if (checkpass.substring(split, split*2) == 'CTF{') {
16          if (checkpass.substring(split*4, split*5) == 'ts_p') {
17           if (checkpass.substring(split*3, split*4) == 'lien') {
18             if (checkpass.substring(split*5, split*6) == 'lz_1') {
19               if (checkpass.substring(split*2, split*3) == 'no_c') {
20                 if (checkpass.substring(split*7, split*8) == '9}') {
21                   alert("Password Verified")
22                   }
```

2) We just join the parts to get the flag.

Flag: picoCTF{no_clients_plz_1a3c89}