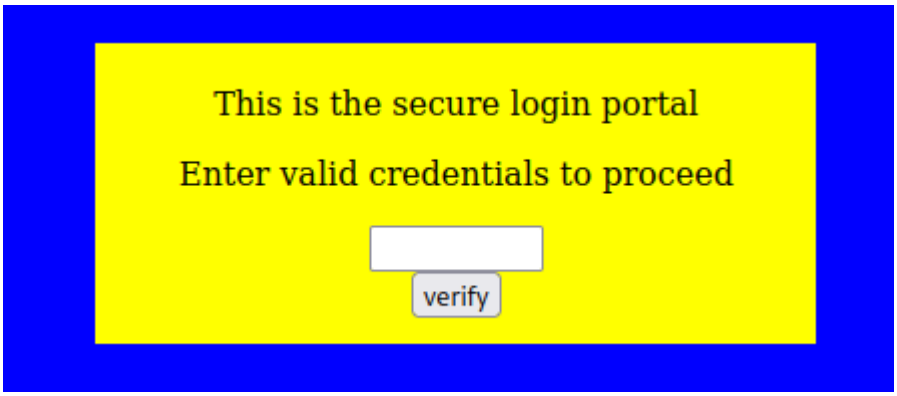
dont-use-client-side

We connect to the website using the link: https://jupiter.challenges.picoctf.org/problem/37821/

The page displays only a login prompt.



By viewing the page source code, we can see a hard coded password verification.

```
<script type="text/javascript">
  function verify() {
    checkpass = document.getElementById("pass").value;
    split = 4;
    if (checkpass.substring(0, split) == 'pico') {
      if (checkpass.substring(split*6, split*7) == 'a3c8') {
        if (checkpass.substring(split, split*2) == 'CTF{') {
         if (checkpass.substring(split*4, split*5) == 'ts_p') {
          if (checkpass.substring(split*3, split*4) == 'lien') {
            if (checkpass.substring(split*5, split*6) == 'lz_1') {
              if (checkpass.substring(split*2, split*3) == 'no_c') {
                if (checkpass.substring(split*7, split*8) == '9}') {
                  alert("Password Verified")
                  }
                }
              }

            }
          }
        }
      }
    }
    else {
      alert("Incorrect password");
    }

  }
</script>
```

We can see that 'split' variable is set to 4.
It appears the code is checking certain substrings.
So, we can see that substring(0, split) == pico
- substring(split, split*2) = CTF{

This means that the first four characters should be 'pico' and the next following set of four characters should be 'CTF{'.
We can then finished the pattern to complete the hardcoded password.

By placing the substrings in the correct order, we get the flag, and can pass the password verification on the website!