

PicoCTF - dont-use-client-side Writeup

Open (<https://jupiter.challenges.picoctf.org/problem/37821>) in Firefox.



This is the secure login portal

Enter valid credentials to proceed



This is the secure login portal

Enter valid credentials to proceed

I inputted random stuff in the input field and clicked "verify".

A dialog appeared after I verified the input field.

When I tried to do the same thing but intercepted with Burp Suite. The Burp Suite didn't catch any response request.

Which mean the verify algorithm worked in a single page.

I Checked the inspector page

```

<html>
  <head> </head>
  <body bgcolor="blue">
    <!--standard MD5 implementation-->
    <script type="text/javascript" src="md5.js"></script>
    <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>
  <div style="position:relative; padding:5px; top:50px; left:38%; width:350px; height:140px; background-color:yellow">
    <div style="text-align:center">
      <p>This is the secure login portal</p>
      <p>Enter valid credentials to proceed</p>
      <form action="index.html" method="post">
        <input id="pass" type="password" size="8">
        <br>
        <input type="submit" value="verify" onclick="verify(); return false;">
      </form>
    </div>
  </div>
</body>
</html>

```

The Javascript ifs looked interesting. There was many parts that looked like parts from the flag. So I tried to arrange the scrambled flag parts in a notepad.

And we got the flag!

Flag: picoCTF{no_clients_plz_1a3c89}