

LinkedIn: [Kelvin Kimotho](#)

dont-use-client-side



Easy

Web Exploitation

picoCTF 2019

AUTHOR: ALEX FULTON/DANNY

Description

Can you break into this super secure portal?

<https://jupiter.challenges.picoctf.org/problem/37821/> ([link](#)) or

<http://jupiter.challenges.picoctf.org:37821>

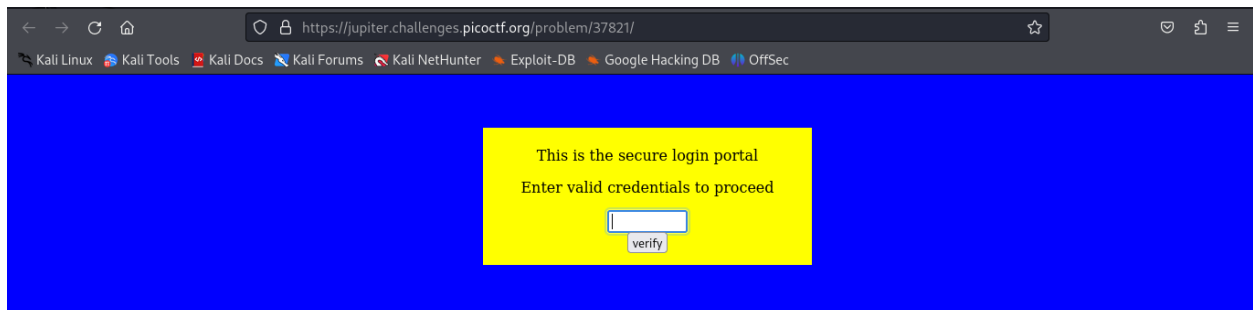
Hints

1

Never trust the client

Solution

I accessed the challenge page and found a form asking for a password. Guessing some common passwords didn't succeed.



I inspected the HTML JS code and found a **verify()** function checking the password client-side.

```
view-source:https://jupiter.challenges.picoctf.org/problem/37821/

1 <html>
2 <head>
3 <title>Secure Login Portal</title>
4 </head>
5 <body bgcolor=blue>
6 <!-- standard MD5 implementation -->
7 <script type="text/javascript" src="md5.js"></script>
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                 }
23               }
24             }
25           }
26         }
27       }
28     }
29   }
30 }
31 else {
32   alert("Incorrect password");
33 }
34 }
35 </script>
36 <div style="position:relative; padding:5px; top:50px; left:38%; width:350px; height:140px; background-color:yellow">
37 <div style="text-align:center">
38 <p>This is the secure login portal</p>
39 <p>Enter valid credentials to proceed</p>
40 <form action="index.html" method="post">
```

I analyzed the password conditions in the JavaScript. I deduced the password based on the conditions which was the flag. **picoCTF{no_clients_plz_1a3c89}**