

## Login picoCTF

login 

 | 100 points 

Tags: picoMini by redpwn Web Exploitation

AUTHOR: BROWNIEINMOTION

Hints 

### Description

(None)

My dog-sitter's brother made this website but I can't get in; can you help?

[login.mars.picoctf.net](http://login.mars.picoctf.net)

31,904 solves / 33,745 users attempted (95%)



88% Liked



 picoCTF{FLAG}

Submit Flag

Upon reading the instructions I opened up the link and saw this web page.

# Login

Username

Password

Submit

I inspected the page and saw that there was src from index.js.

```
1 <!doctype html>
2 <html>
3   <head>
4     <link rel="stylesheet" href="styles.css">
5     <script src="index.js"></script>
6   </head>
7   <body>
8     <div>
9       <h1>Login</h1>
10      <form method="POST">
11        <label for="username">Username</label>
12        <input name="username" type="text"/>
13        <label for="password">Password</label>
14        <input name="password" type="password"/>
15        <input type="submit" value="Submit"/>
16      </form>
17    </div>
18  </body>
19 </html>
```

I put the js code through a beautifier so that it would be easier to read.

```

1 (async () => {
2     await new Promise((e => window.addEventListener("load", e))), document.querySelector("form").addEventListener("submit", (e => {
3         e.preventDefault();
4         const r = {
5             u: "input[name=username]",
6             p: "input[name=password]"
7         },
8         t = {};
9         for (const e in r) t[e] = btoa(document.querySelector(r[e]).value).replace(/=/g, "");
10        return "YwRtaW4" !== t.u ? alert("Incorrect Username") : "C6ljB9NURns1M3J2M3JfNTnydJNyxZuZcnyZc181M3J2M3JfNTnydJNyrQ"
11        !== t.p ? alert("Incorrect Password") : void alert(`Correct Password! Your flag is ${atob(t.p)}.`);
12    })
13})();

```

From reading to code I can see that the desired username and password were given so I copied and pasted them into the website but unfortunately, it was not the correct implementation.

# Login

Username

YWRtaW4

Password

.....|

Submit

Upon doing further research on what the strings I decided to use popular operations on cyberchef. The first one I tried was converting from base 64 which proved to be the correct implementation. The username converted to admin and the long string for the pw was the flag.

Recipe

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

Input

cGljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ

Output

|picoCTF{53rv3r\_53rv3r\_53rv3r\_53rv3r\_53rv3r}