



**LinkedIn:** [Kelvin Kimotho](#)

login






Medium

Web Exploitation

picoMini by redpwn

AUTHOR: BROWNIEINMOTION

Hints 

Description

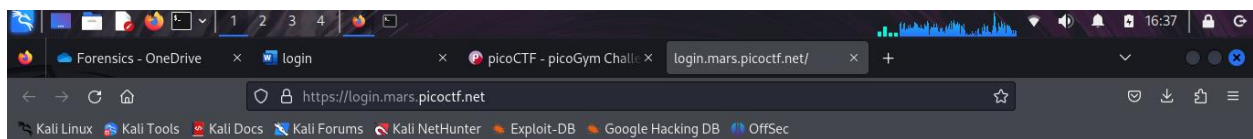
(None)

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

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

## Solution

This site rendered a login page that requires the user to enter a **username** and a **password** to login successfully, unfortunately i had no valid credentials.



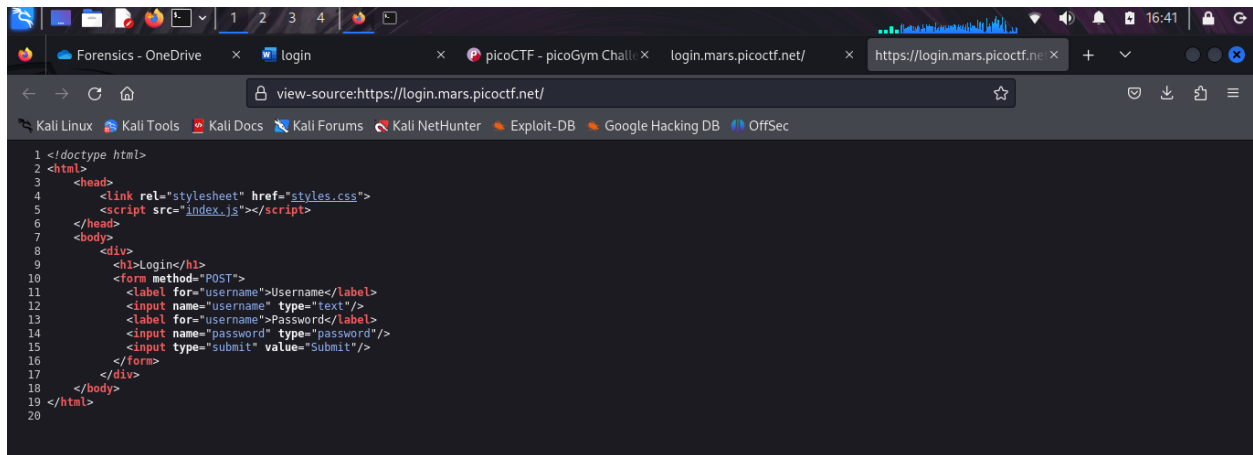
### Login

Username

Password

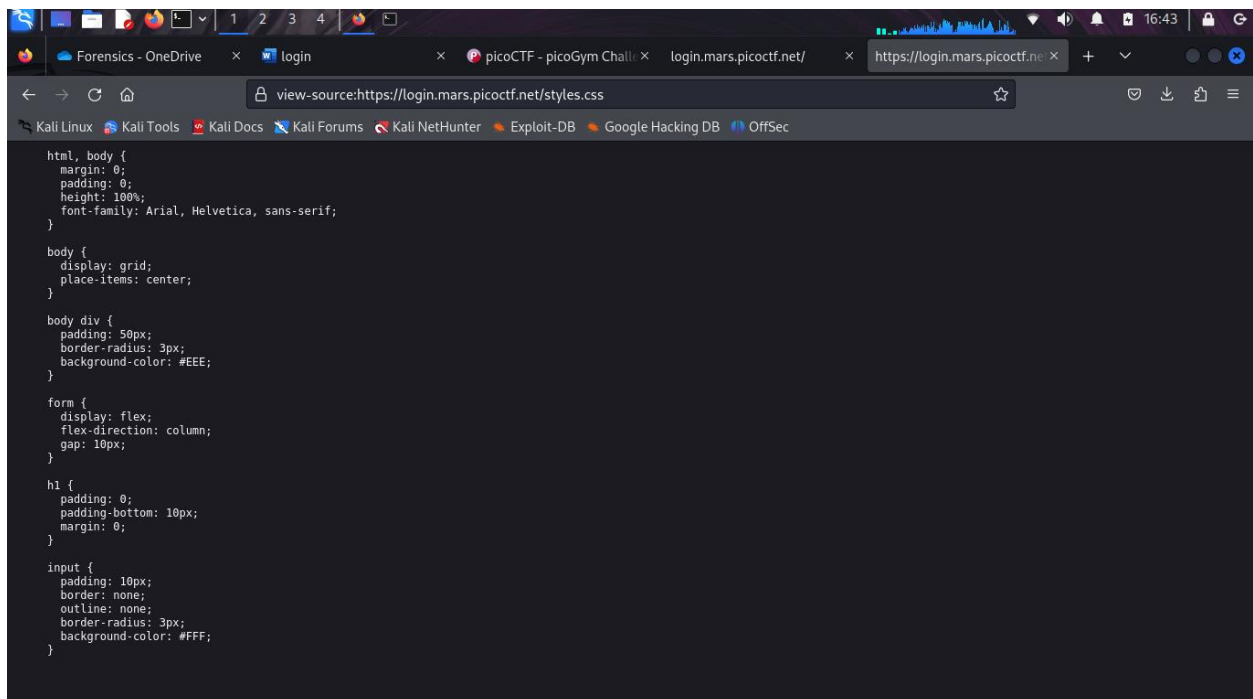
Submit

I went ahead looking for '**vulnerabilities**' that would allow me in. I began by examining the page html source code but i found no credentials left.



```
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>
20
```

I discovered **styles.css** and **index.css** files. I examined the css code but found no credentials.



```
html, body {
  margin: 0;
  padding: 0;
  height: 100%;
  font-family: Arial, Helvetica, sans-serif;
}

body {
  display: grid;
  place-items: center;
}

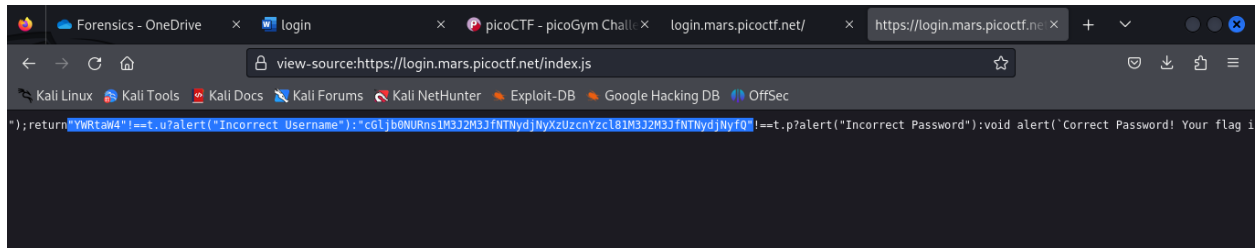
body div {
  padding: 50px;
  border-radius: 3px;
  background-color: #EEE;
}

form {
  display: flex;
  flex-direction: column;
  gap: 10px;
}

h1 {
  padding: 0;
  padding-bottom: 10px;
  margin: 0;
}

input {
  padding: 10px;
  border: none;
  outline: none;
  border-radius: 3px;
  background-color: #FFF;
}
```

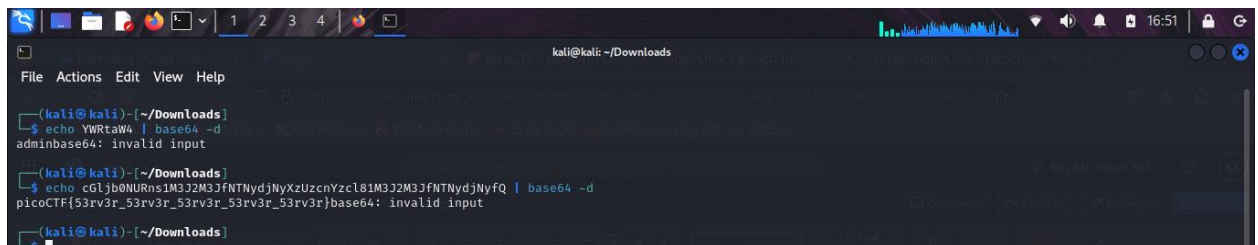
On examining the **index.js** file, I discovered that the user input was supposed to match various string the username was supposed to match **YWRtaW4** while the password was to match **cGljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ**.



The username and password strings appeared to be base64 encodings, I tried decoding them and this is what i discovered.

**YWRtaW4** gave **admin** as the username while

**cGljb0NURns1M3J2M3JfNTNyYdjNyXzUzcnYzcl81M3J2M3JfNTNyYdjNyfQ** gave **picoCTF{53rv3r\_53rv3r\_53rv3r\_53rv3r\_53rv3r}** as the password.



I tried login in with the credentials and i succeeded retrieving the flag

**picoCTF{53rv3r\_53rv3r\_53rv3r\_53rv3r\_53rv3r}**

