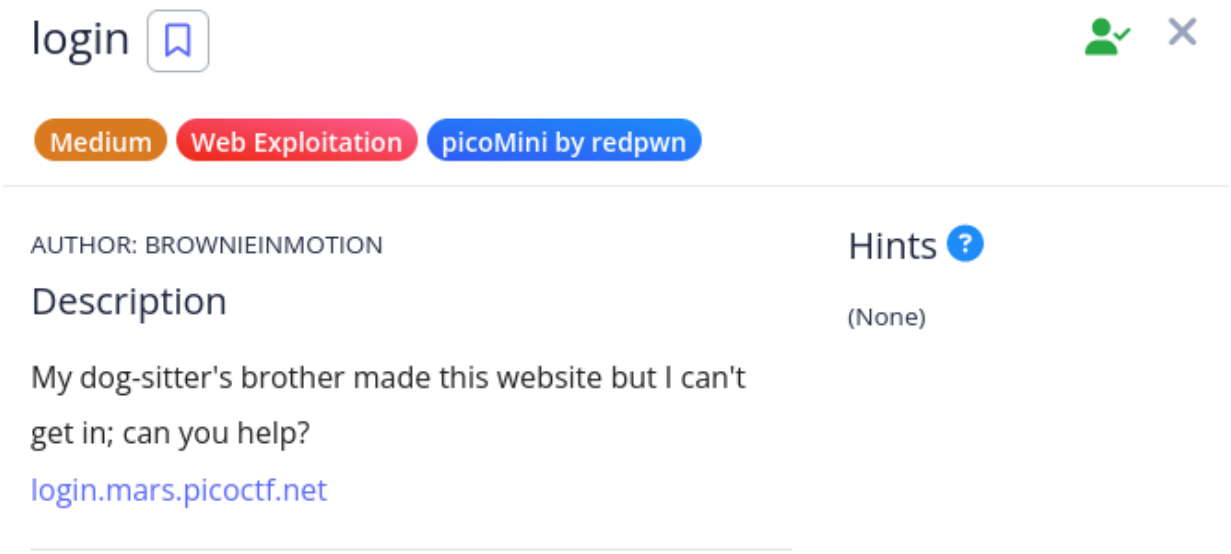
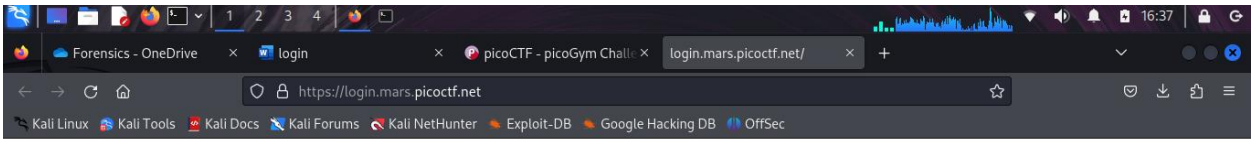
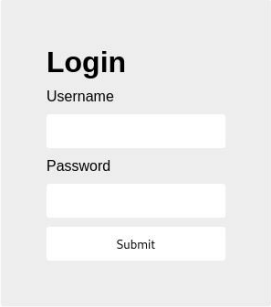
LinkedIn: Kelvin Kimotho



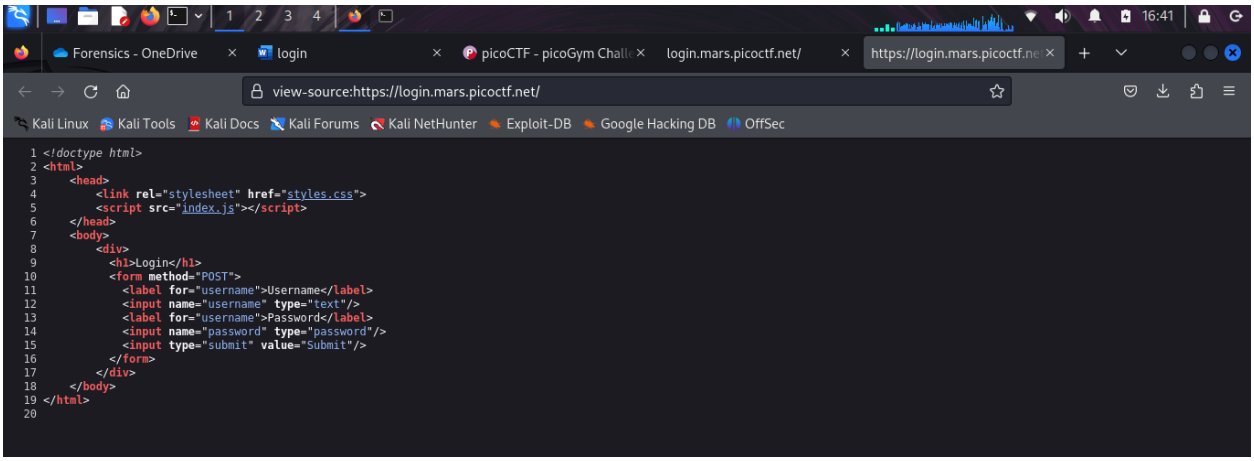
Solution

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.

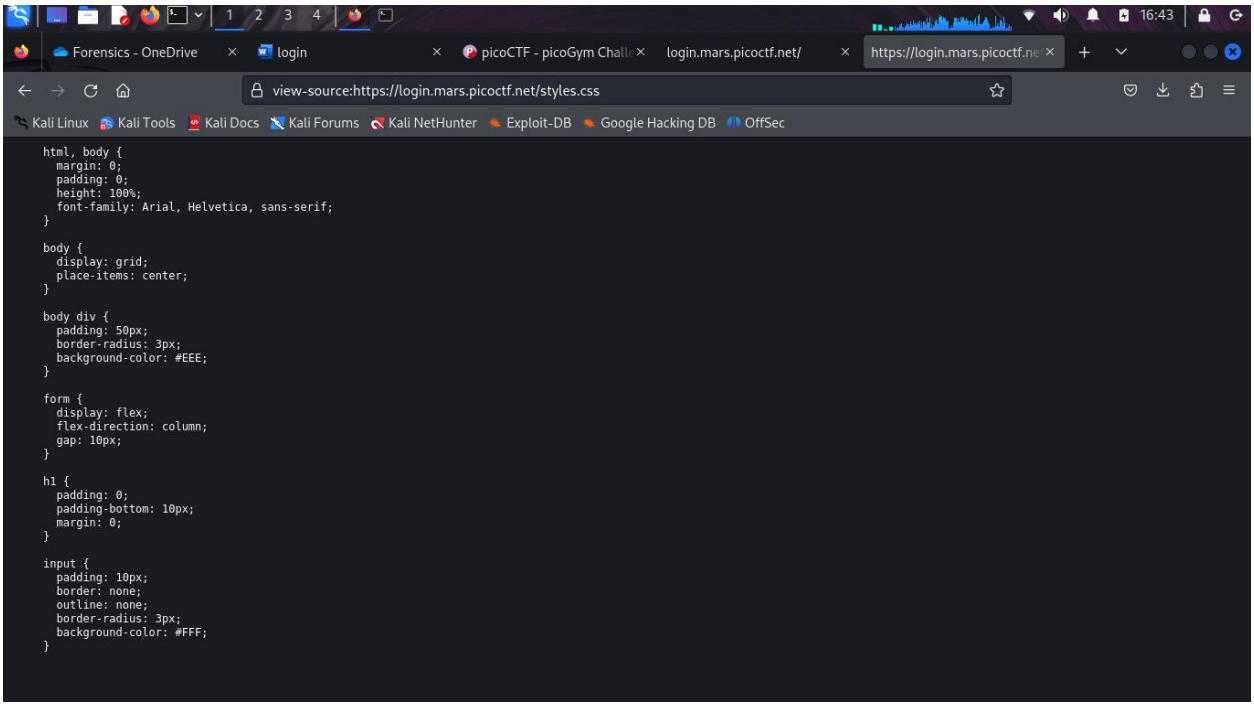




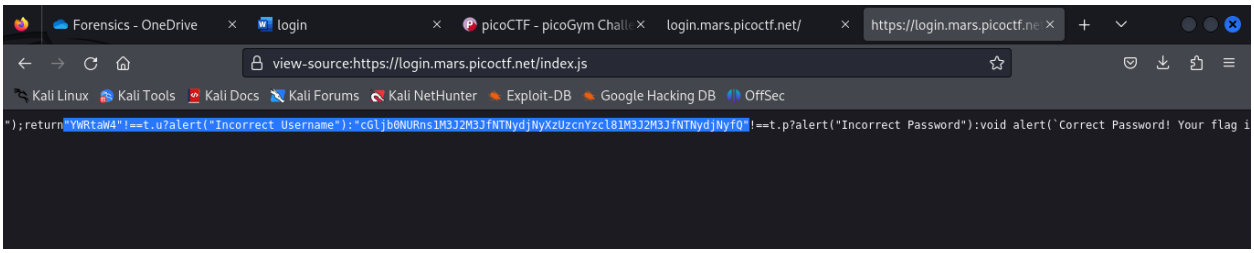
I went ahead looking for 'vulnerabilities' that would allow me in. I began by examining the page html source code but i found no credentials left.



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



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 cGljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ 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}