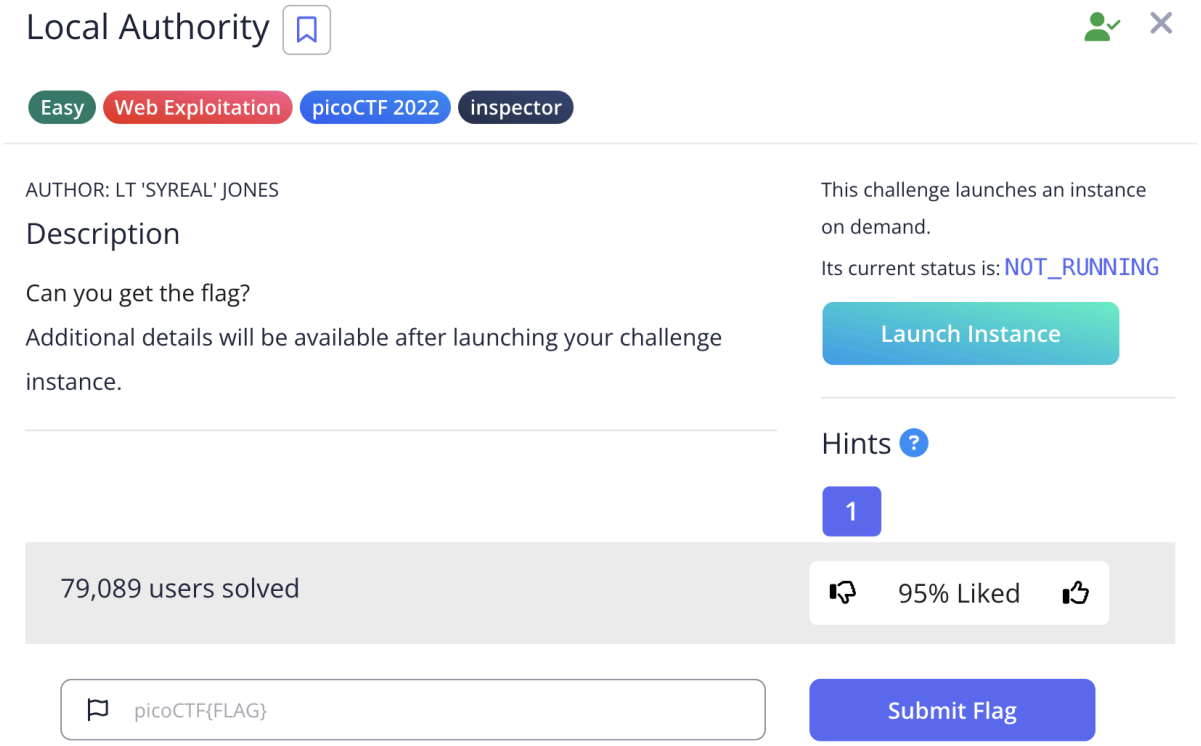
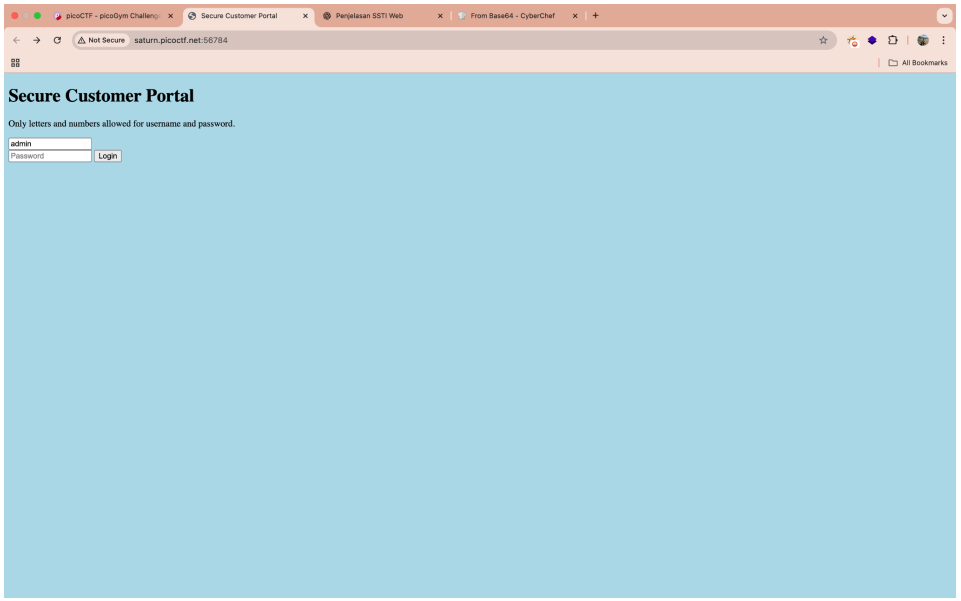


Hint :

1. How is the password checked on this website?

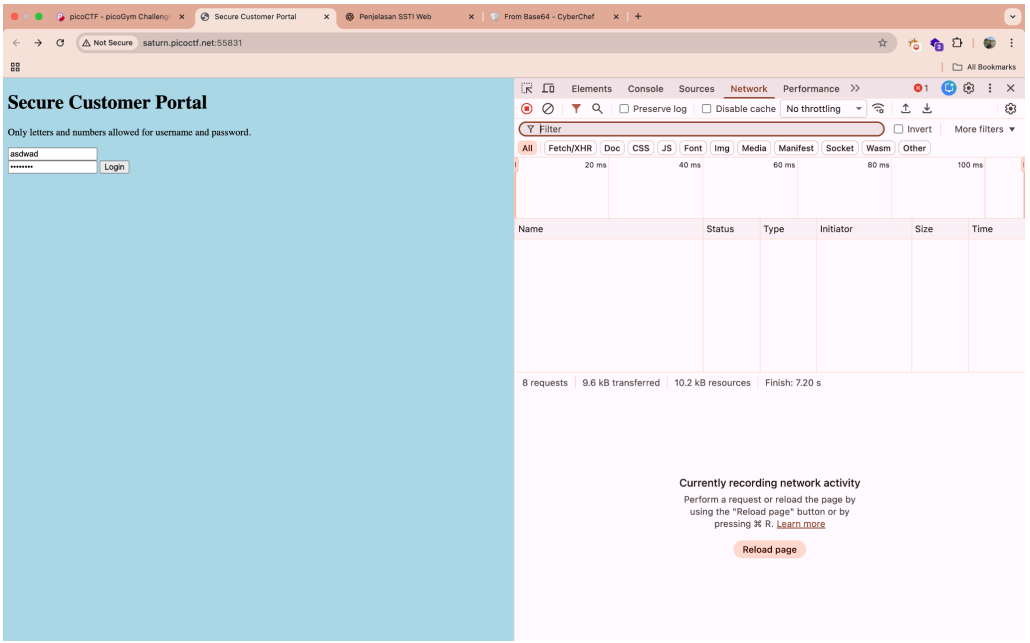
Solusi :

Kita coba untuk launch instance, setelah launch instance akan ada link web yang dituju dengan tampilan berikut.

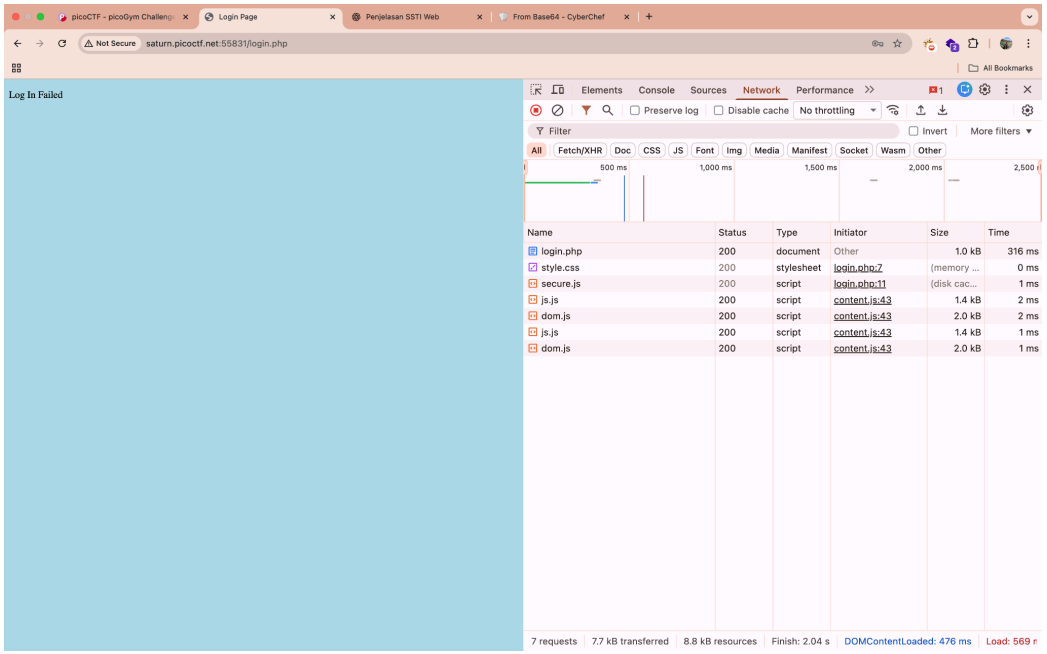


Web ini berisi form username dan password untuk diinput (login), dan bayangan kita mengacu pada injeksi SQL, namun ketika lihat hint, kami menyadari bahwa hint tersebut menginstruksikan kita untuk dapat mengerti cara password login ini dicek.

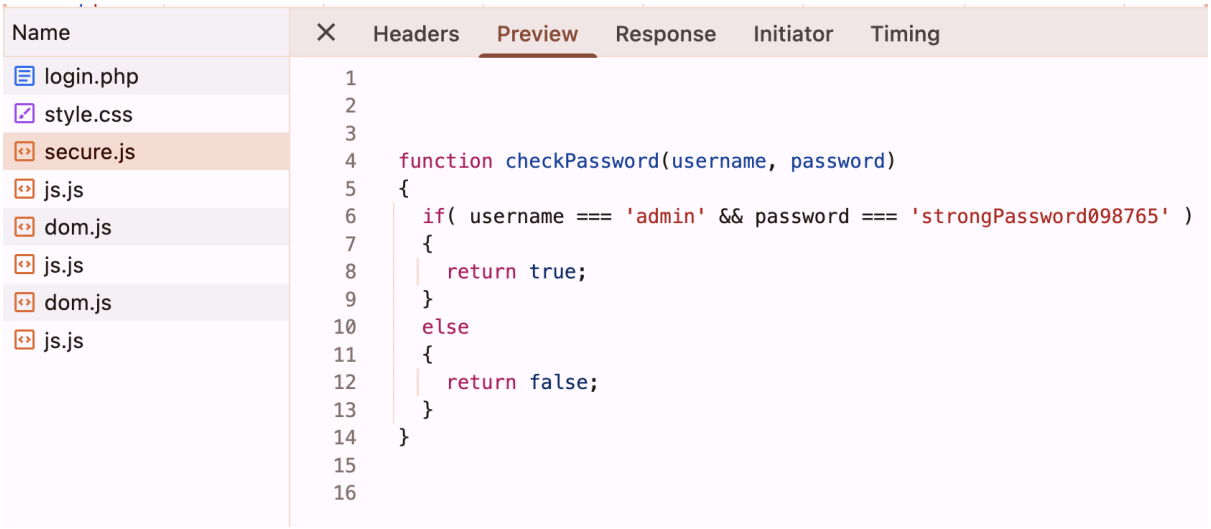
Kami coba untuk langsung inspect sebelum mensubmit username dan password untuk memicu perubahan pada program di inspect.



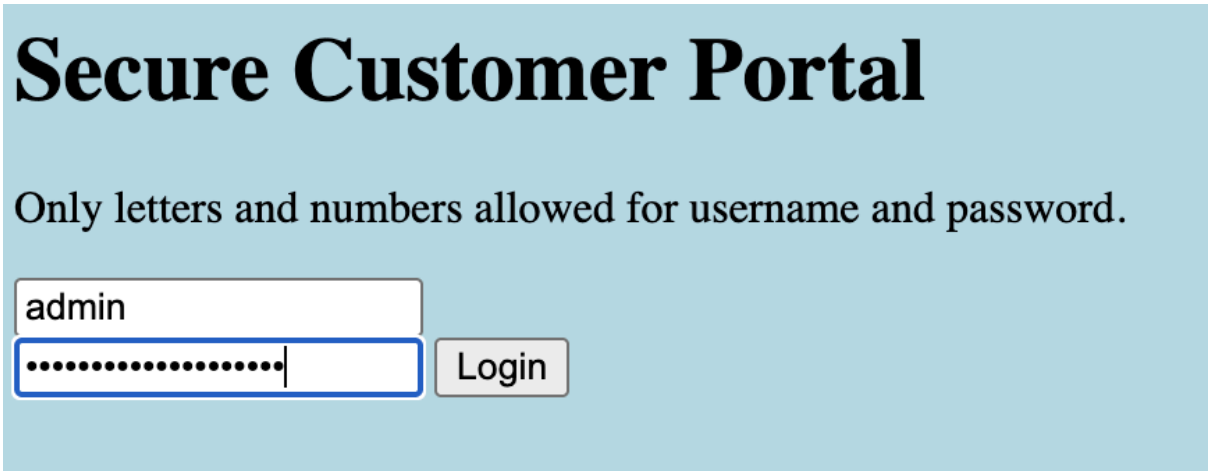
Ini adalah tampilan page ketika belum mensubmit username dan password yang ada pada form.

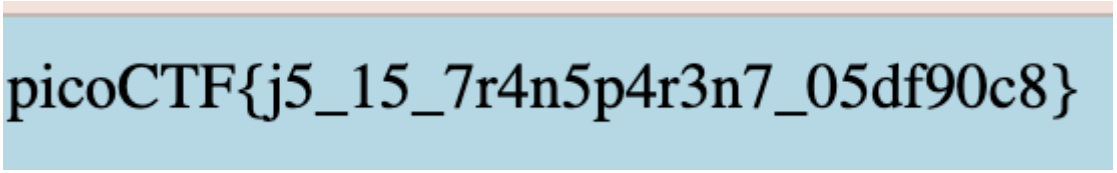


Setelah dilakukan submit, network memberikan beberapa file js dan kami terpacu pada file secure.js, langsung saja kita buka.



Dan ternyata disana terdapat validasi username dan password beserta isi username dan password dengan role sebagai admin. Jadi kita coba input saja di form login tadi.





Benar saja, kami menemukan flagnya.