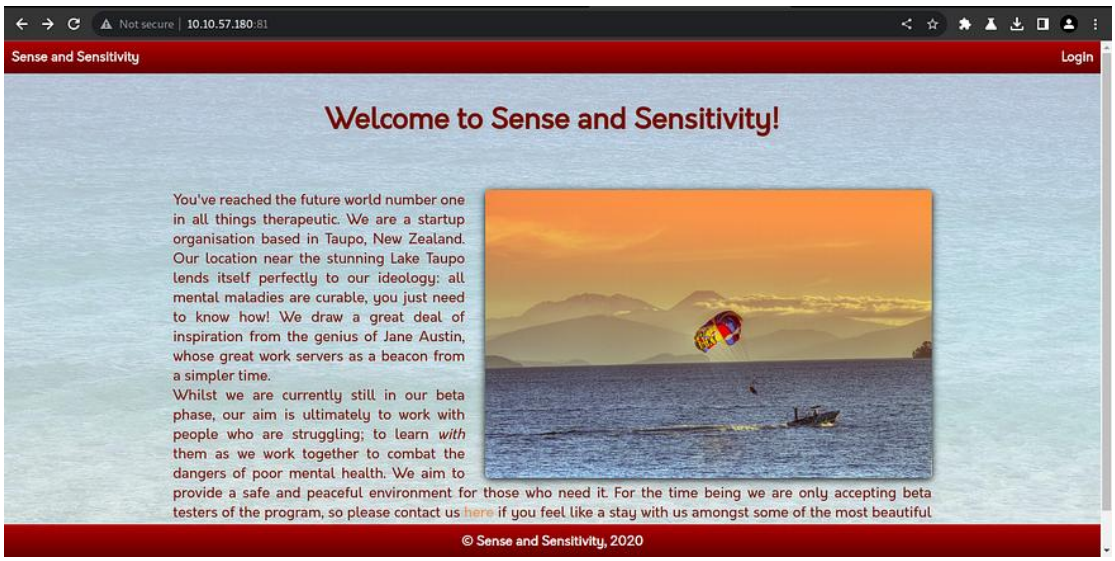
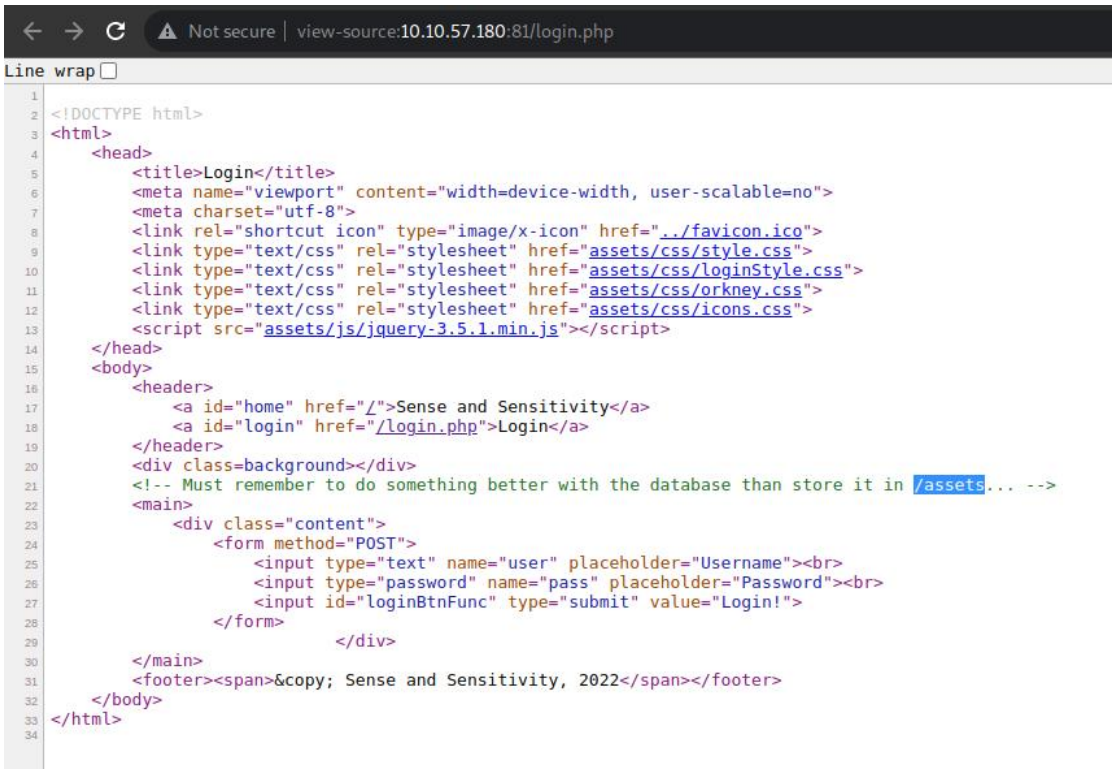
Task 8 : Cryptographic Failures (Challenge)

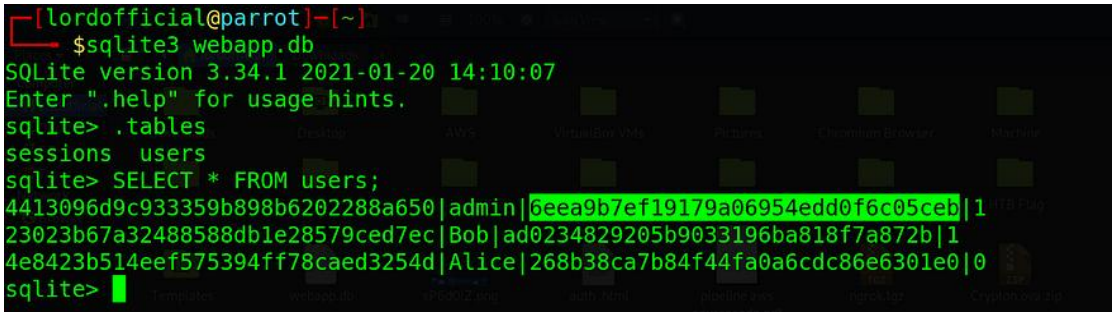
It's now time to put what you've learnt into practice! For this challenge, connect to the web application at http://machine-ip:81/.

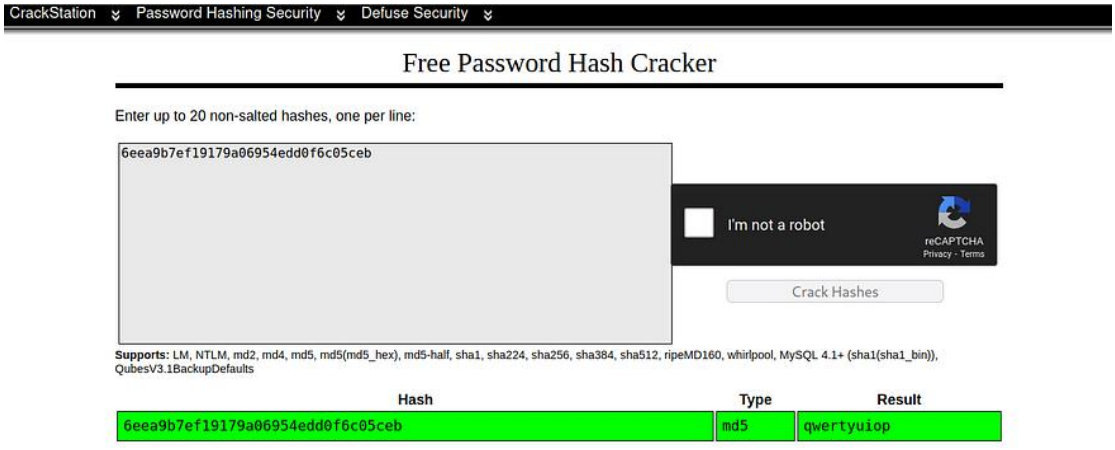


Go to login page and view the source code to find the hidden directorty.

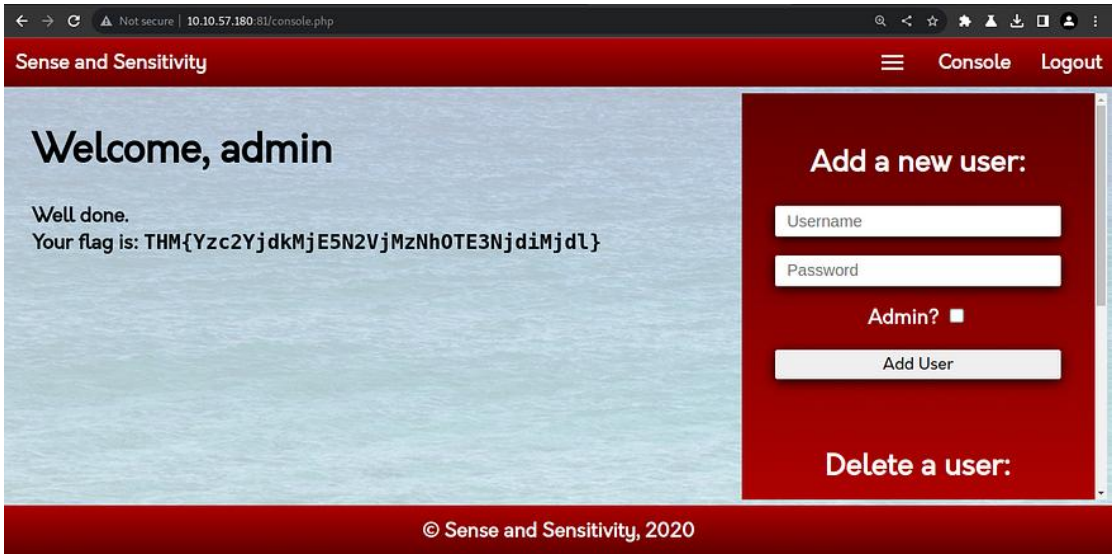


Download the webapp.db to examine it





After Cracking the hash Now login as admin to get the flag.



Answer the questions below :

Have a look around the web app. The developer has left themselves a note indicating that there is sensitive data in a specific directory.

1. What is the name of the mentioned directory?
A. /assets

2. Navigate to the directory you found in question one. What file stands out as being likely to contain sensitive data?
A. webapp.db

3. Use the supporting material to access the sensitive data. What is the password hash of the admin user?
A. 6eea9b7ef19179a06954edd0f6c05ceb

4. Crack the hash.
What is the admin's plaintext password?
A. qwertyuiop

5. Log in as the admin. What is the flag?
A. THM{Yzc2YjdkMjE5N2VjMzNhOTE3NjdiMjdl}