Task 17 : Identification and Authentication Failures Practical

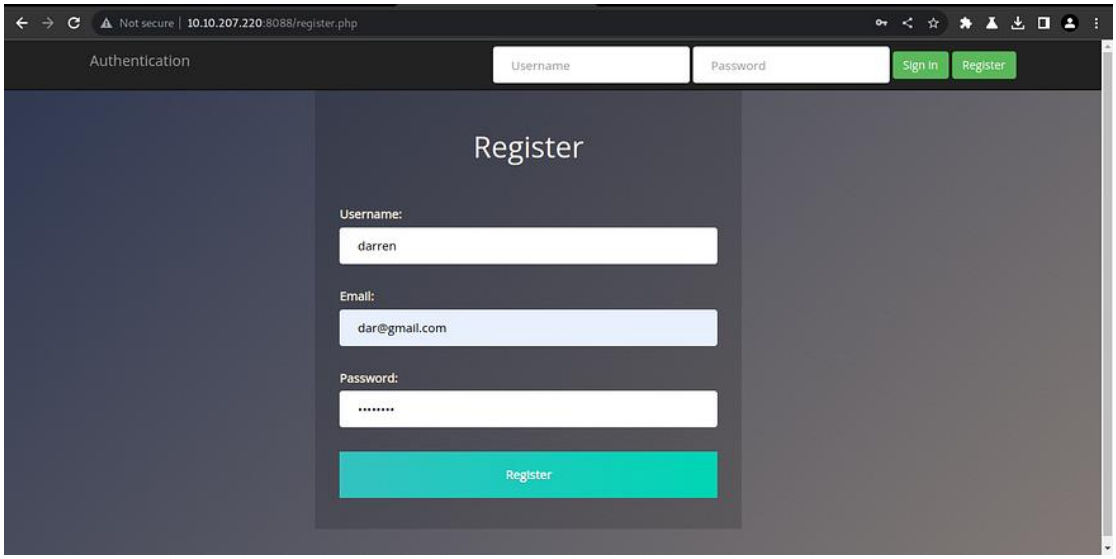
For this example, we'll look at a logic flaw within the authentication mechanism.

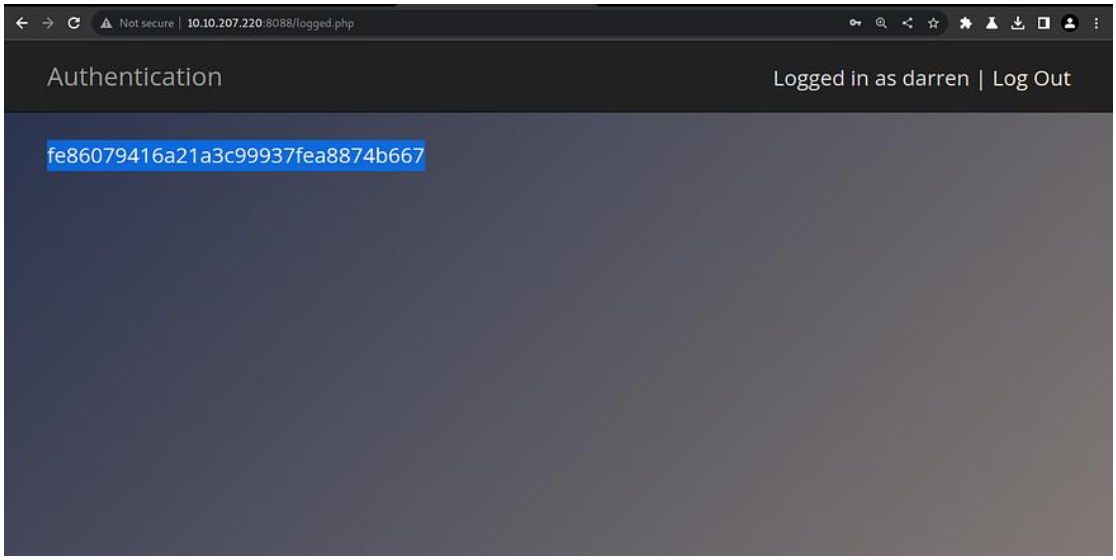
Many times, what happens is that developers forget to sanitise the input(username & password) given by the user in the code of their application, which can make them vulnerable to attacks like SQL injection. However, we will focus on a vulnerability that happens because of a developer's mistake but is very easy to exploit, i.e. re-registration of an existing user.

Let's understand this with the help of an example, say there is an existing user with the name admin, and we want access to their account, so what we can do is try to re-register that username but with slight modification. We will enter " admin" without the quotes (notice the space at the start). Now when you enter that in the username field and enter other required information like email id or password and submit that data, it will register a new user, but that user will have the same right as the admin account. That new user will also be able to see all the content presented under the user admin.

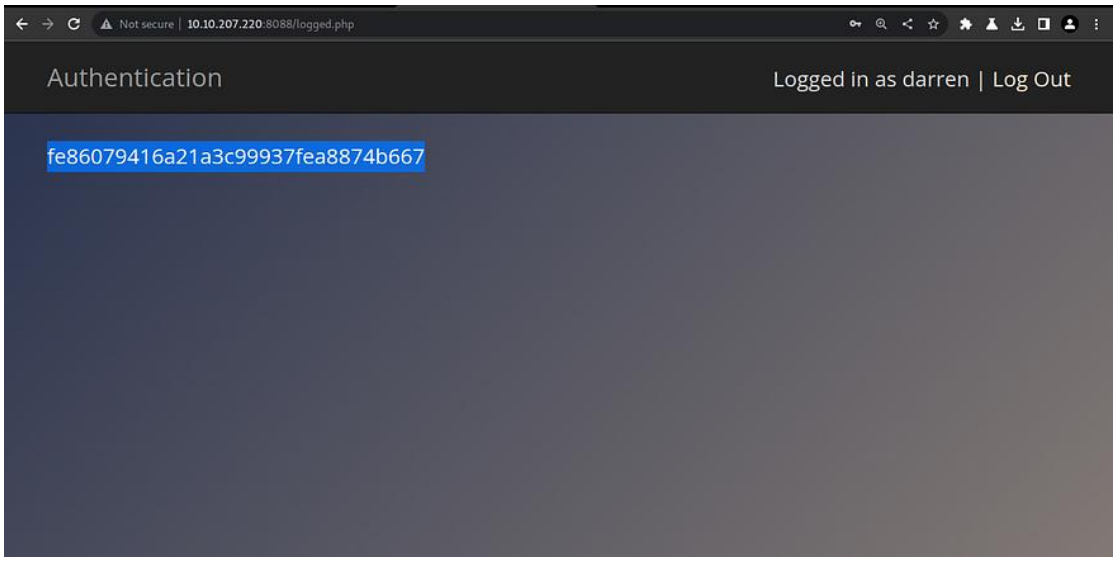
To see this in action, go to http://10.10.30.59:8088 and try to register with darren as your username. You'll see that the user already exists, so try to register " darren" instead, and you'll see that you are now logged in and can see the content present only in darren's account, which in our case, is the flag that you need to retrieve.

To register give a single space before darren and try to login using same .





To register give a single space before arthur and try to login using same.



Answer the questions below :

1. What is the flag that you found in darren's account?
A. fe86079416a21a3c99937fea8874b667

2. Now try to do the same trick and see if you can log in as arthur.
A. No answer needed

3. What is the flag that you found in arthur's account?
A. d9ac0f7db4fda460ac3edeb75d75e16e