**IDOR in Password Reset Form**

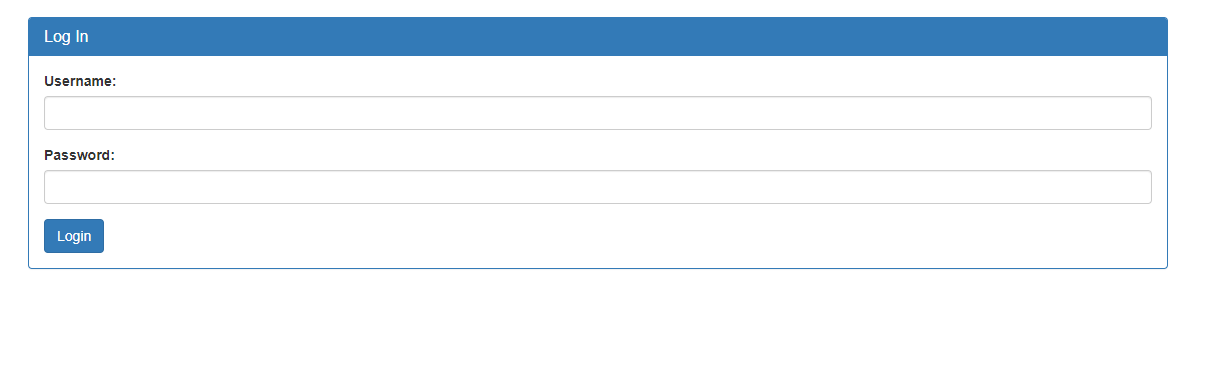
Irish-Name-Repo 1

Vulnerability Description:

The vulnerability lies in the database. So, entering the payload in the login credential we can get the flag.

Summary:

As in the given hint, we need to check the users which are used in the database. So, we need to login as admin. Using the payload as username we can get the flag easily.

This is the login credential

Using the username: ‘OR 1=1 --

We can directly login as the admin, NO NEED OF PASSWORD

And logging in as ADMIN will give the flag.



So, the flag is: picoCTF{s0m3\_SQL\_c218b685}