Challenge 3

http://192.168.2.11/sqli/sql3/ [Level: Advanced]

- Bypass authentication and provide the flag id

  The blacklisting does not allow comment characters. So you cannot inject # or --. The SQL Query looks like this:

  Select * from users where username='input1' and password='input2'

  Remember password field is not vulnerable (as per the logic in previous challenge). When you inject the payload ' or '1'='1 in username the query becomes:

  Select * from users where username='' or '1'=1' and password='input2'

  The AND operator has precedence over OR, so the query will be evaluated as:

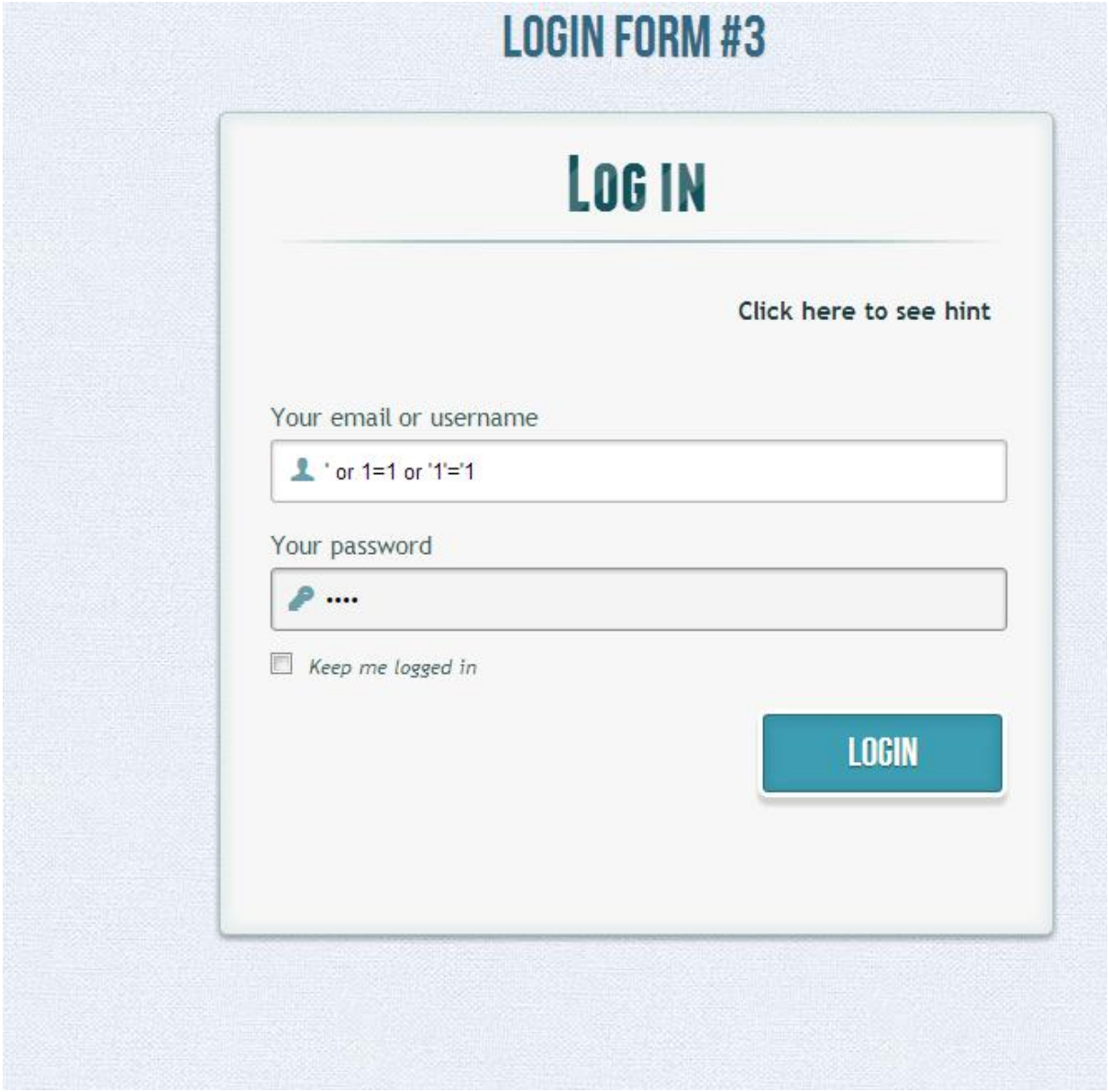
  Select * from user where FALSE or [*TRUE and FALSE]*

  Which will eventually return:

  FALSE or FALSE

  Thus the query will evaluate as FALSE and not return any rows:

  By Injecting another Boolean operator (OR clause) we can change the execution to return TRUE



Username: ‘ or 1=1 or ‘1’=’1

Password: anything