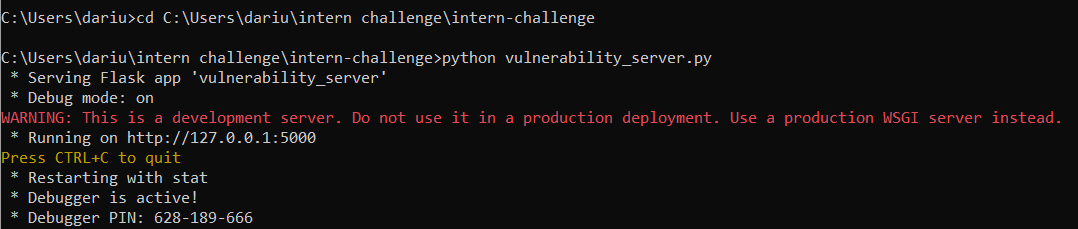
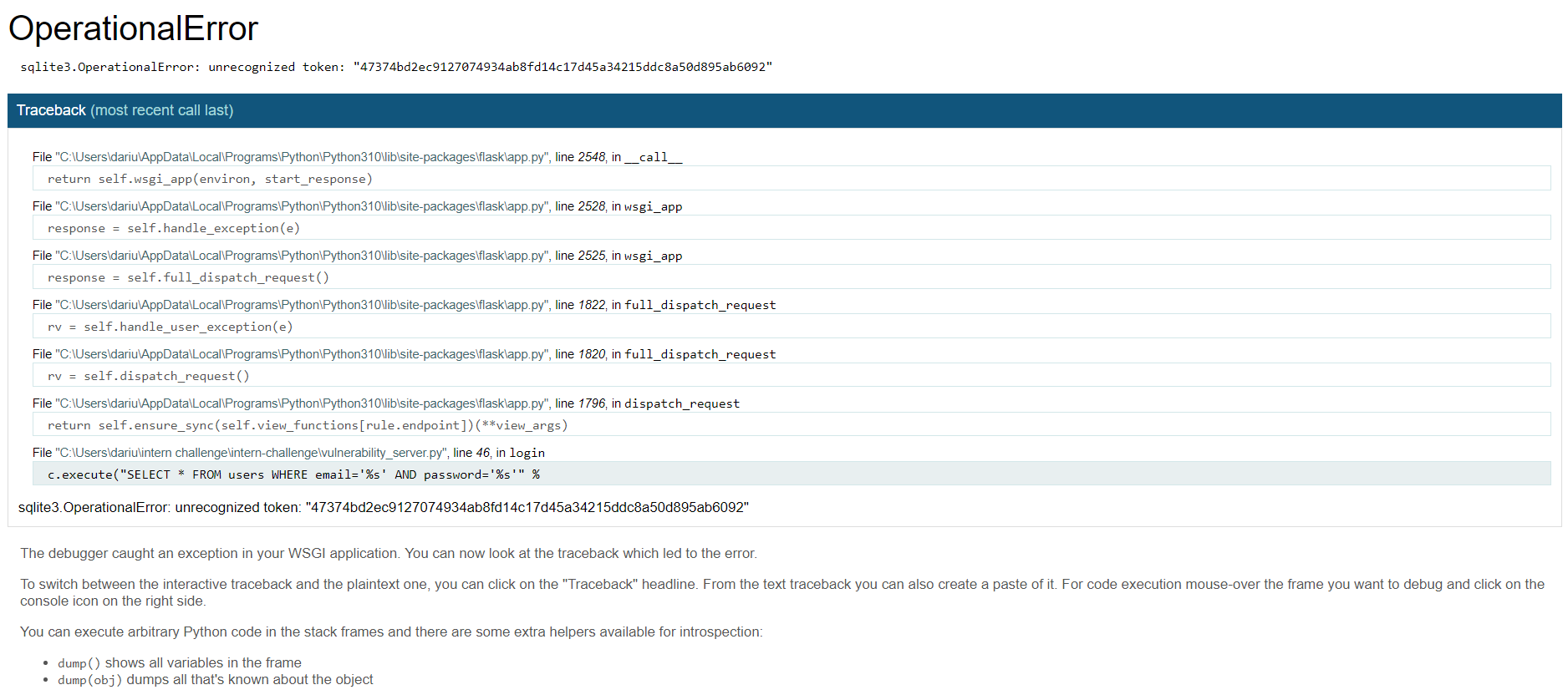
Firstly, set up all the required things such as Flask and downloading the repository

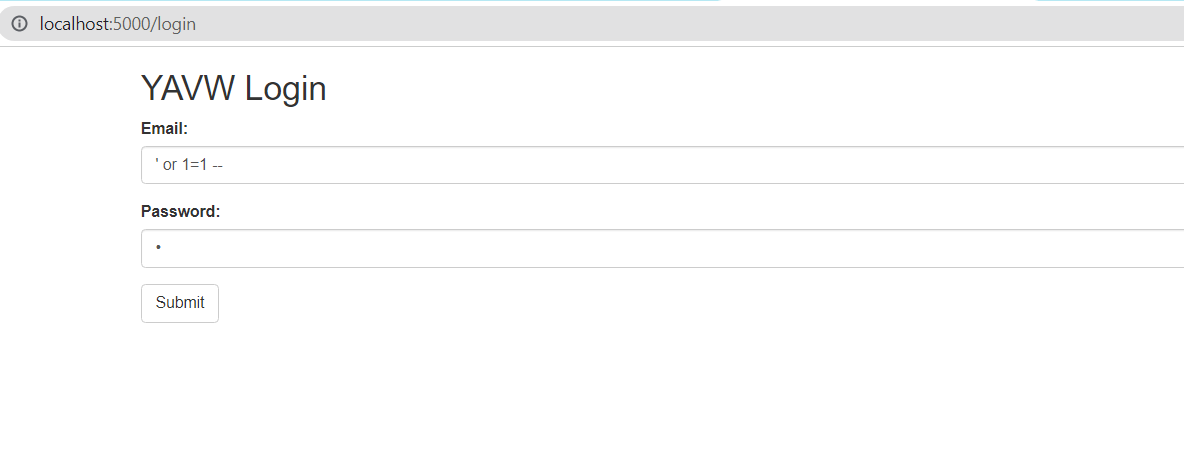
Run the python script in command prompt to enable the localhost server

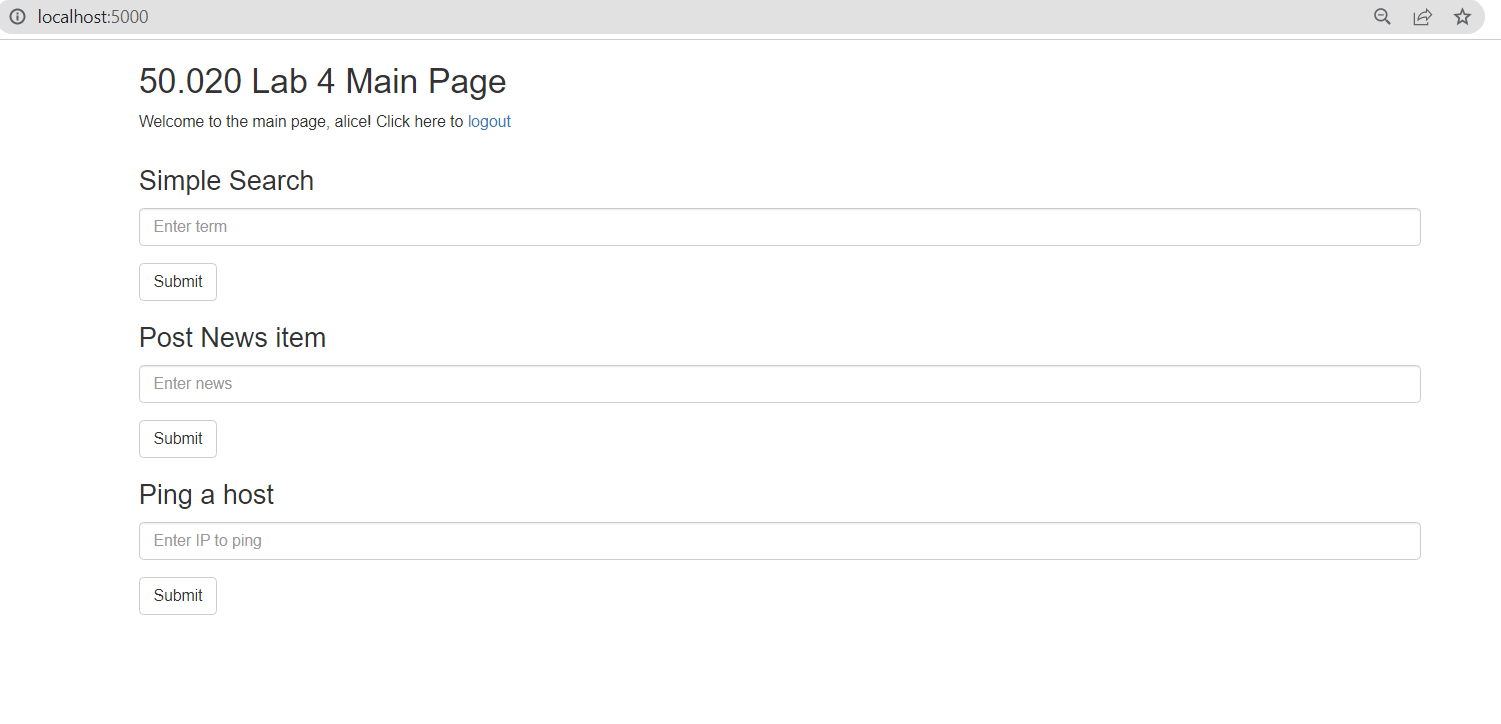


Before starting, enter “ ‘ “ into any of the input fields and see whether an error message is given, if it is, we will be able to perform sql injection as we can see the select query statement



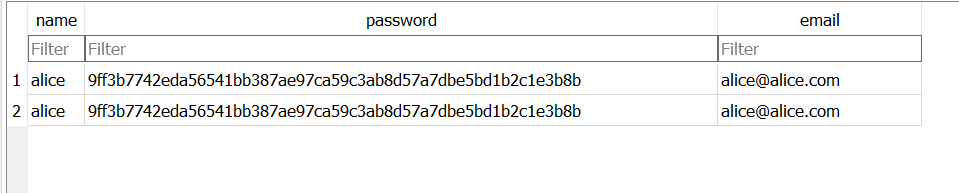
Once we are inside the login page, type in the following and you will be able to login as alice



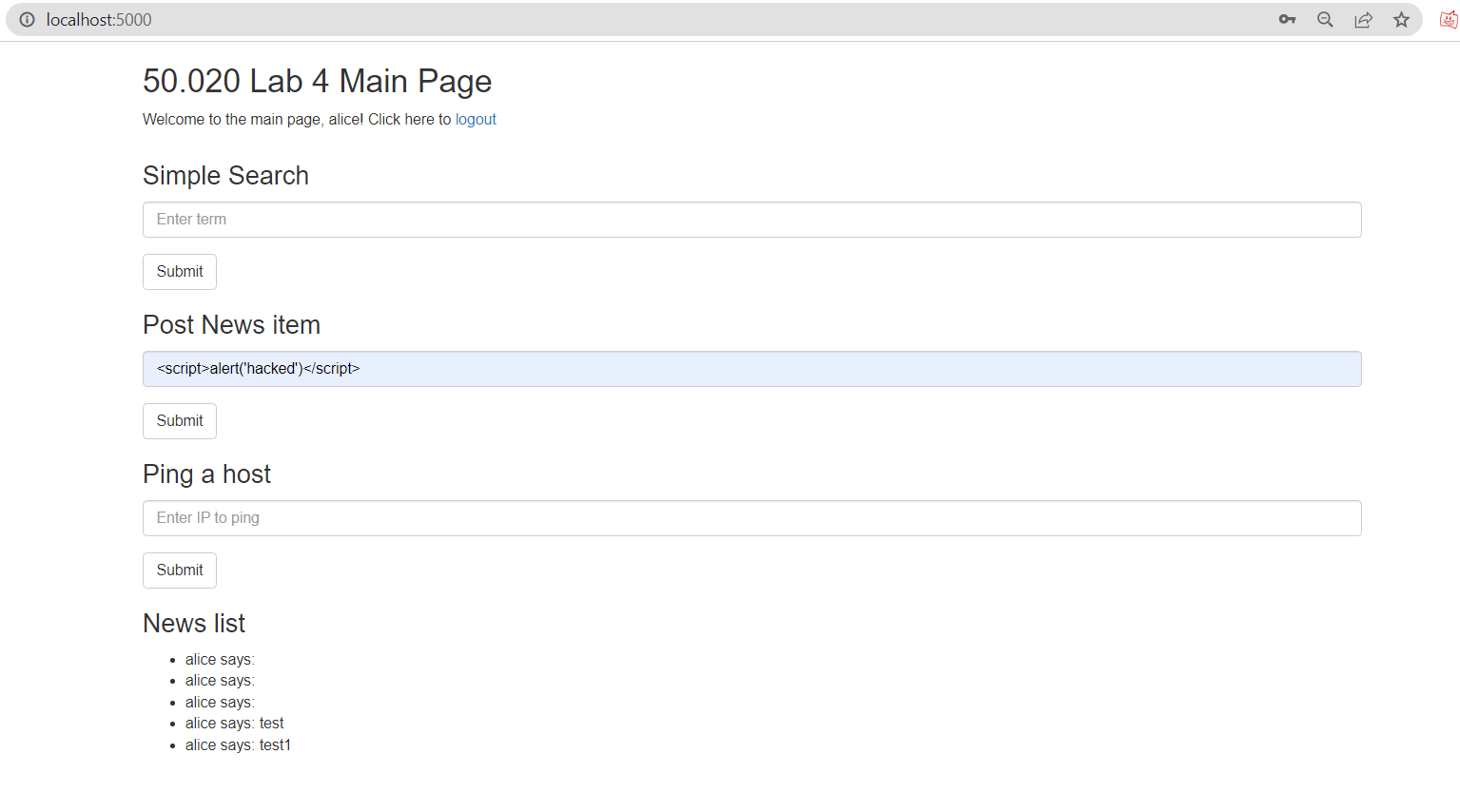


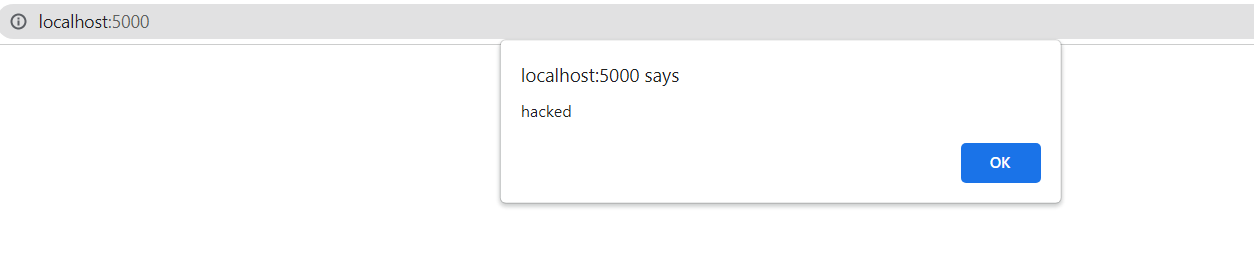
' or 1=1 – enables us to login without knowing the password because “ – “ makes the query statement ignore everything behind it which is the password portion, therefore enabling us to login as alice

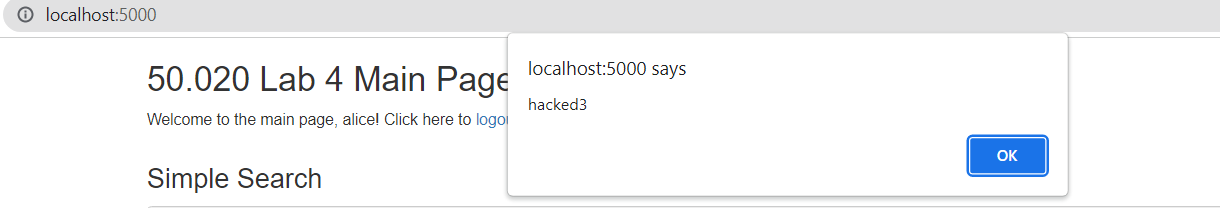
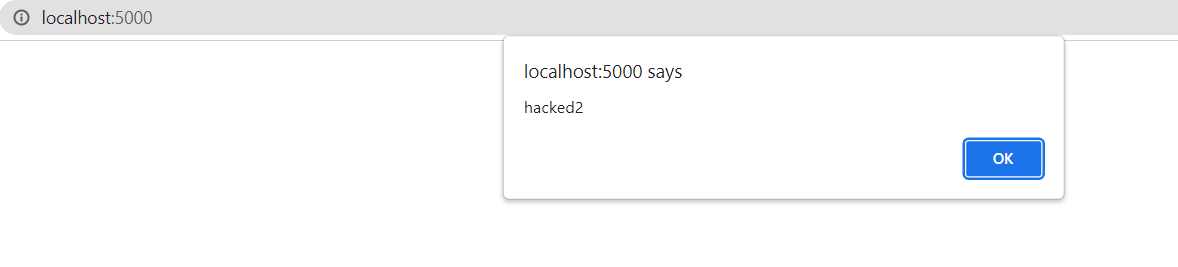
However, I was able to see the encrypted password of alice inside the database, but could not decode it as it has multiple layers of encoding



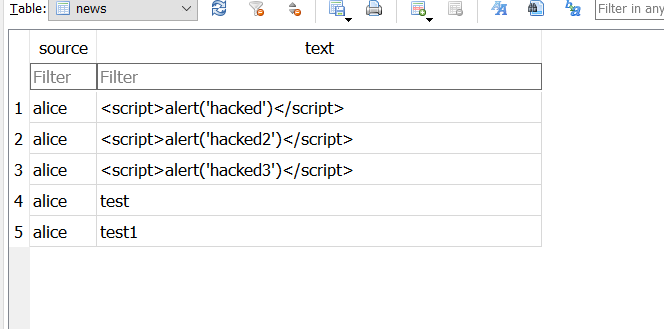
In order to perform a persistent xss attack, we can input javascript into the database, by typing what is seen in the news input, there will always be an alert whenever the user refreshes as well as closing and opening this webpage



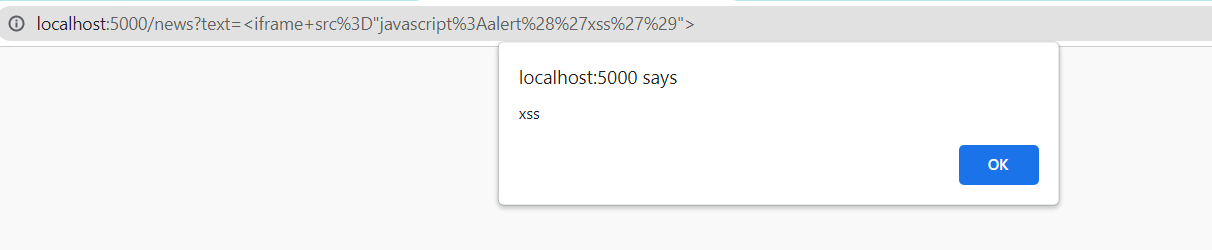


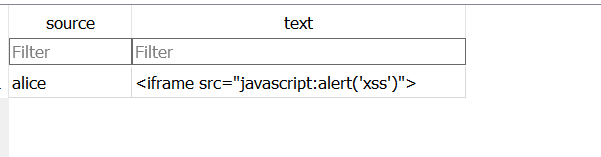


This will be stored in the database as well, hence making it persistent



If we want to use html instead, we can type <iframe src="javascript:alert('xss')">





However, I have tried using html and javascript to perform persistent xss but only the html alert is showing up

