WebGoat SQL Injection Assignment 3

3. Retrieving all data from user_system_data table and Dave's password

Steps

- From the problem description, I noticed how the user_system_data table is structured.
- This gave details about the column names and how the first command of the query will be structured: user_name'
- The hint was also helpful. So, I learned how to use special character * to append statements in sql from lesson 2.
- Since we are interested in retrieving Dave's information and in fact this is the only username available to us from the user_system_data table, the first command is Dave'
- After different trial, I arrived at a solution: **Dave'; SELECT * FROM user_system_data;--** This command shows the data in columns USERID, USER_NAME, PASSWORD, COOKIE.
- Then we are able to retrieve the password of Dave as: **passW0rD**.
- Another possible command: **Dave' SELECT * FROM user_system_data WHERE user_name = 'dave'--**
- I came about this after different manipulation of the error message.

5. Trying to Login as Tom

Steps

- I went through the lesson 4 and learned about blind sql injection.
- I opened WebGoat on ZAP because I had to monitor the response from the server according to the hint.
- I found out that registering a new user and re-registering it again, will either be TRUE or FALSE.
- I registered a new user evidence' and '1'='1 which is TRUE
- Then I tried re-registering with the same credentials but with '1'='2 and paid close attention to the server reply as the hint indicated.
- Then from lesson 4, I decided to compared the substring of the password with different alphabet, which was exhausting. I used this command: tom' and substring(password,1,1)='t'-- which worked. So 't' is the first letter. Then I did a walk through different on alphabet randomly, while keeping note of the alphabet I already tested like a brute force attacker.
- After different permutations of different alphabets, I arrived at the password: '**thisisasecretfortomonly**'. It was not easy.