# Penetration Testing

Research as much as you can about the following types of hackers:

|  |  |
| --- | --- |
| White Hat Hacker |  |
| Grey Hat Hacker |  |
| Black Hat Hacker |  |

During the first lesson we did some hacking (Brute Force & DDoS). What kind of Hacker were we?

**Extension: What are the legal implications for each? Could they be punished? Could they go to prison?**

# SQL Injection

You’re now going to try performing some SQL Injection.

Head over to <https://stormy-oasis-27277.herokuapp.com>

1. Open up the Console. On Chrome click the 3 dots (top right) -> More Tools -> Developer Tools. This should open up a window. Along the top of that window one of the options is Console. This should have some messages on it.
2. Enter a random username and password guess e.g. username: abc, password: 123. What console messages can you see? For each login attempt you should see 2 messages. Type them out here:
3. One of those messages should look like an SQL Query. Imagine that it was written in python cause that’s a bit easier to understand:

userUsername = input(“Enter a username”)

userPassword = input(“Enter a password”)

**if username = userUsername and password = userPassword:**

print(“Login success”)

else:

print(“Incorrect Username/Password”)

1. Now we need to change this code so that the if statement will pass. Imagine the userUsername was something like ‘# commented’

The # is a comment in python so it would comment out the rest of the line for us.

i.e. **if username = ‘**#*commented’ and password = userPassword*:

Now we need to do the same in SQL to turn the query into something that will pass.

Find out how to do comments in SQL. Try putting in a username followed by a comment. How does that change the query?

1. You might notice one problem with the query (HINT: Look at ‘). Try and fix it.
2. Now we’re very close and you’ll hopefully have a query like:

SELECT \* FROM Users WHERE UserId = 'abc'

But our problem is that we sadly don’t know any usernames. And the username abc doesn’t work.

# Password Verification

Now I want you to Write a Program in Python that allows a user to set a username and password and then allow them to login.

1. The user should be asked to user a username. You should store whatever they enter.
2. The user should then be asked to enter a password. You should store whatever they enter. But their password must also meet the following critera:
   1. 8+ Letters
   2. Contain a Number
   3. Contain both an upper-case character and a lower-case character.
   4. Contain one of the following special characters: ! @ £ $ % & \* € ~ < >
   5. The user should be repeatedly asked to re-create this password until they have met the above criteria. Once it meets the criteria then they can continue.
3. Then you should welcome to user to the app saying “Welcome”.
4. Then you should ask them for their username.
5. Then ask for their password.
6. Compare the user entered username and password with the one they set up earlier:
   1. If they’re the same, then print out “You’ve successfully logged in”
   2. If they’re different, then print out “Login Failed – Try Again”

**Extension: How can you improve the security of the Login? We’ve discussed several ideas in class. Can you implement one of them in your program?**