Readme file: Python code solutions to solve/mitigate security issues

Appointment and scheduling management information system (ASMIS)

Queens medical centre

Security implementation 1 - Hashing passwords with pbkdf2_hmac

Storing password in plaintext would allow easy access for an attacker to apply a combination with matching usernames to login into the account. Therefore, in the solution-provided passwords are set up to apply hashing with pbkdf2_hmac, which encodes a provided password that is safe for database storage.

Please refer to code line # 75-84 and # 211 – 217 in Login.py

Password-Based Key Derivation Function 2 (PBKDF2) is a salt and 100,000 iterations of the Secure Hash Algorithm 256-bit hash (SHA-256). This is currently considered as one of the best options for password hashing and is recommended in US National Institute of Standards and Technology (NIAST) Special Publication 800-132 (Reitz & Schlusser; 2016).

Security implementation 2 – Account lockout policy: Failed login attempt limitation

As an overwhelming number of failed logins indicates a possibility for an attacker to try repeatedly searching correct credential, and "maximum-number-of-failed-login-attempts = 3 failed attempts" configuration is enabled to restrict such danger (OWASP, n.d).

Please refer to code line # 138-160 in Login.py

However, a security feature with limited failed login attempts could also allow an attacker to lock out many different users on purpose (Hasan, 2017), impacting daily operational use of ASMIS. Nonetheless, such a situation sends an alert on such attacks, enabling ASMIS administration take necessary actions.

Security implementation 3 – Password strength controls

Following password strength controls have been applied to make it improbable to guess the password.

- Password Length - minimum 8 characters & maximum 20 characters.

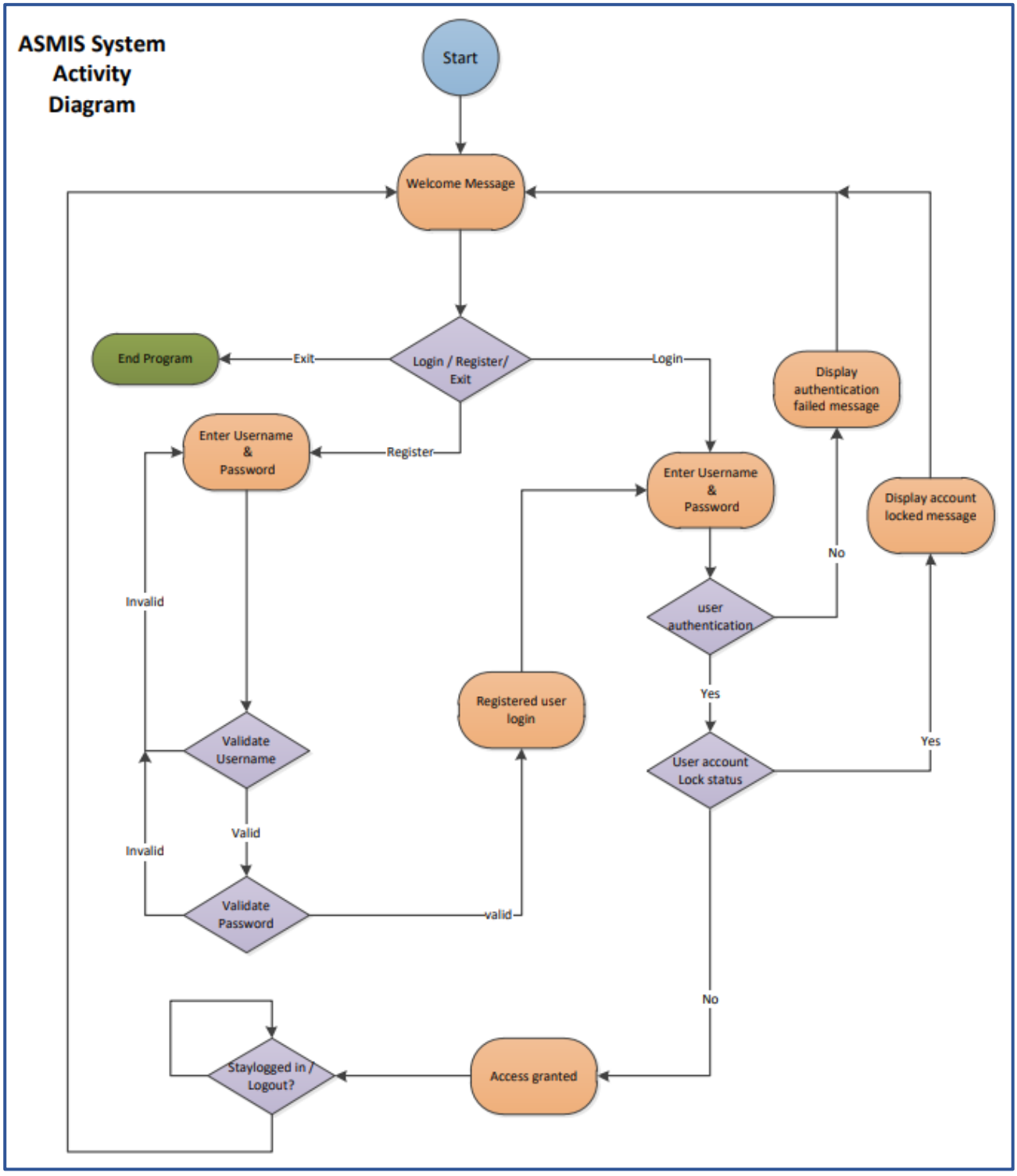
  US National Institute of Standards and Technology (NIAST) considered shorter than 8 characters password as week (OWASP, n.d). The maximum password length is used to prevent long password Denial of Service Attacks on the server, which may lead to the website becoming unresponsive (OWASP, n.d).

- A mixture of both uppercase and lowercase letters
- A mixture of letters and numbers
- The inclusion of at least one special character, e.g., ! @ # ?]

Please refer to code line # 89-110 in Login.py

ASMIS System Access Process

Figure 1 – Activity diagram



Database structure

Database name: ASMIS

Table: usertable

Table attributes within the database structure are as follows

Figure 2 – Database structure

```
mysql> SHOW COLUMNS FROM usertable;
+-------------+-------------+------+-----+---------+-------+
| Field       | Type        | Null | Key | Default | Extra |
+-------------+-------------+------+-----+---------+-------+
| username    | varchar(10) | NO   | PRI | NULL    |       |
| salt        | tinyblob    | YES  |     | NULL    |       |
| password    | tinyblob    | YES  |     | NULL    |       |
| failedcount | smallint(6) | YES  |     | NULL    |       |
+-------------+-------------+------+-----+---------+-------+
4 rows in set (0.00 sec)
```

Supported Python libraries:

```
1    import mysql.connector
2    import uuid
3    import hashlib
4    import os
5    import re
6    import getpass
7    import stdiomask
```

How to access the system

User Registration

- New username must have minimum 6 characters and maximum 10 character, without an ability to use blank space as a username
- Inability to take existing username for new user registration

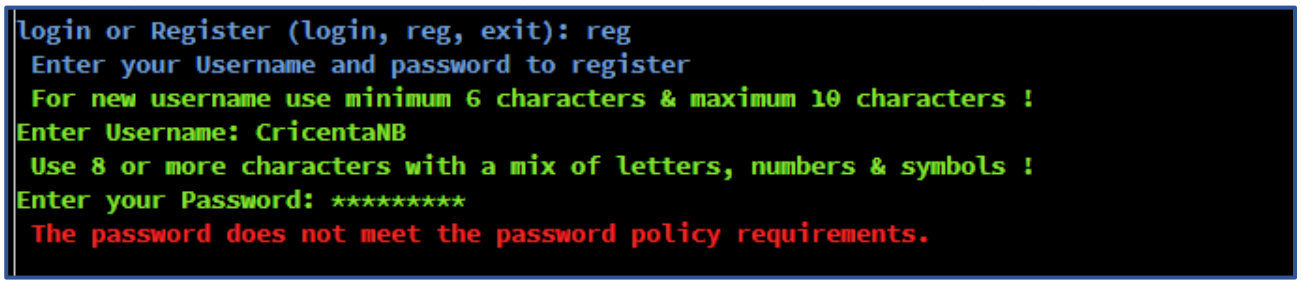
```
Last login: Sat Dec 12 20:57:42 2020 from 192.168.10.156
codio@manual-float:~/workspace$ python3 Login.py
  Welcome to the ASMIS System

login or Register (login, reg, exit): reg
 Enter your Username and password to register
 For new username use minimum 6 characters & maximum 10 characters !
Enter Username: CricentaB
 Use 8 or more characters with a mix of letters, numbers & symbols !
Enter your Password: **********
 Username was already taken. Please select another
 Enter your Username and password to register
 For new username use minimum 6 characters & maximum 10 characters !
Enter Username: CricentaS
 Use 8 or more characters with a mix of letters, numbers & symbols !
Enter your Password: **********
 User Registration Successful please login  !!!!!!!!!!!!!!
```

Security implementation 1 - Hashing passwords with pbkdf2_hmac in the database

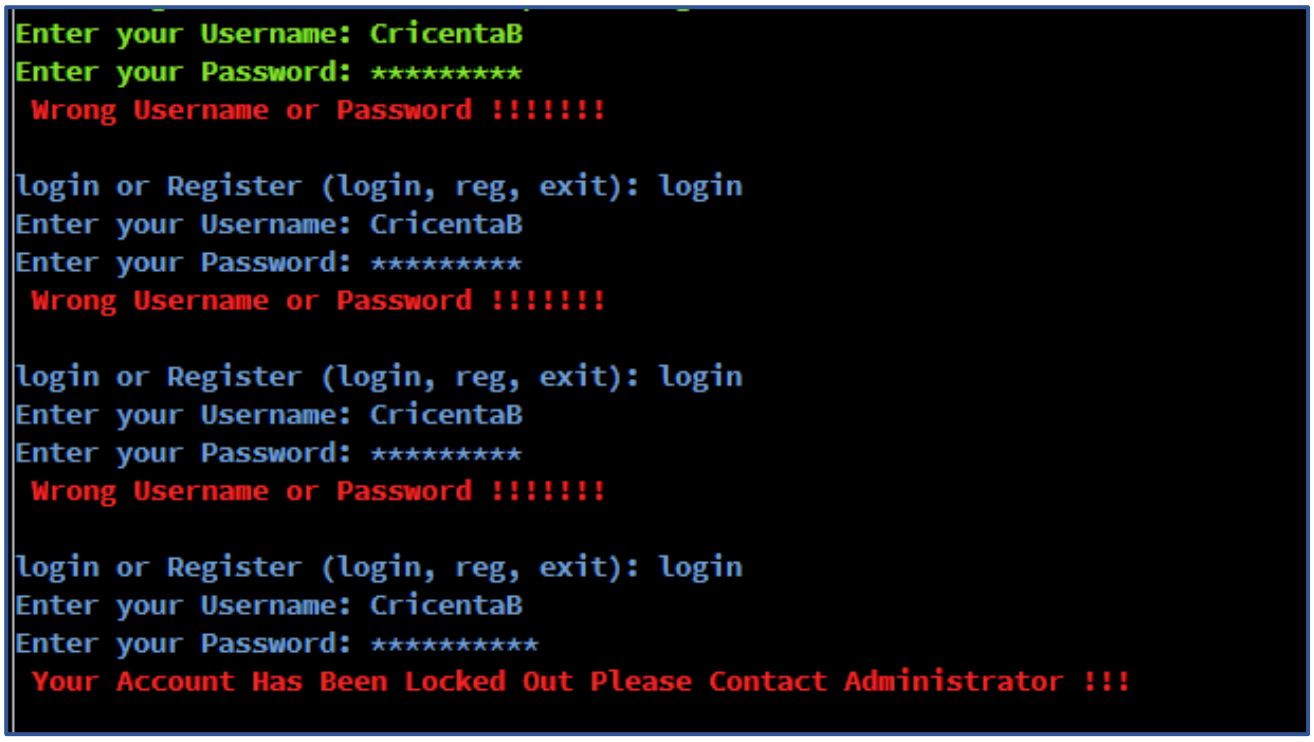
```
mysql> select * from usertable;
+------------+----------------------------------+----------------------------------+-------------+
| username   | salt                             | password                         | failedcount |
+------------+----------------------------------+----------------------------------+-------------+
| AdminASMIS | ?g??8??r?lh?.??/?G??w?
                                  ??                  | w?.????D??xĚV??qt?       ?GkB3
    |           1 |
| CricentaB  | ?????qu???73????Knr
                              B?D                 | =?i??n???R??x????k??|??                    |
     3 |
?F?/?G              |           0 |?m?n??n                    | sM??x?L???T??s.?
?????F9??a?|??~?7_??                |          0 |
| Nuwan_1983 | h?Fr#JO`?.?bX]Uaq?K+?xn
                                  ?          | ?0????[???C??I??8???/r?=?R??#                          |
        0 |
?_ioK?|??&             |           0 | ?bS??             | ?]0?S@?Q???C?zG?
| sebastian  | ??^?M?8?K?,87?B?z?5?8%?             | ?t??i ??BH??j!2~?d? C?N??n?              |
   0 |
| Sujith1983 | ?qVC?k5?s????vQ?I´?2<?% ?             | ??嗇??R??{m      ???MC`??
                                                                        ??T?I??
  |           3 |
+------------+----------------------------------+----------------------------------+-------------+
8 rows in set (0.00 sec)
```

Security implementation 3 – Password strength controls according to the password policy



User Login

Security implementation 2 – Account lockout policy: Failed login attempt limitation – 3 attempts



Reference list

Hasan, A. (2017) *How can hackers try so many password combinations when hacking an account, while most websites limit login attempts??* Available from: https://www.researchgate.net/publication/314171322_How_can_hackers_try_so_many_password_combinations_when_hacking_an_account_while_most_websites_limit_login_attempts [Accessed 10 December 2020].

OWASP. (n.d.) *Authentication Cheat Sheet*. Available from: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html [Accessed 10 December 2020].

Reitz, K. & Schlusser, T. (2016) *The Hitchhiker's Guide to Python - Best Practices for Development*. 1st ed. California: O'Reilly Media, Inc.