This python code to achieve a solution for the Appointment and Scheduling Management Information System (ASMIS) for Queens medical center. The web-based system as per the individual essay, may facing cyber threats such as spoofing, elevation of privilege, and denial of service.

To mitigate those cyber threats, will use techniques such as authentication and authorization in this python code to prevent those threats.

Authentication: for ASMIS system the user will start with login process. User should to login successfully to the system before doing any function such as booking an appointment or cancel a booked one, otherwise, user have to register as a new user and apply these two conditions (username is a new and not exist – password is not short and easy, it should be more than 6 digits). In python code these done by executing these methods login(), user\_exist(), pass\_check(), and register().

Authorization: after authentication process, this time to determine if this authenticated user is authorized to access or perform system actions (Phillips et al., 2016). No access without a validate login and applying level of access for the user to restrict the access to the functions of the system. In ASMIS system, user can not access the system without login process. In addition, during the registration stage the least privilege level will be applied which is (0), this level defined as to authorize the user to book a new appointment and panned the change or cancel the appointment. If the level of privilege is (1) which is a higher level, the user or staff could change or cancel the appointment. In python code these done by register() and is\_authorized() functions.

Moreover, encryption technique is applied in python code to encrypt the user password and to store it encrypted in the DB, plain text password may cause data exposure if the DB accessed by an authorized person. Using hashlib.sha265 function to encrypt the password before storing to reduce the chance of knowing it or stealing (Phillips, 2018).

Finally, applying technique to limit the failed login to three times for the same user may prevent the user to try to guess the password and may mitigate denial of service attack. Menu\_login() function is the responsible to limit the user failed login trying in the python code.

References

Phillips, D. (2018) *Python 3 object-oriented programming: Build robust and maintainable software with object-oriented design patterns in Python 3.8*. 3rd ed. Birmingham, UK: Packt Publishing. Available from: https://books.google.com/books?hl=en&lr=&id=08t1DwAAQBAJ&oi=fnd&pg=PP1&dq=Python:+Master+the+Art+of+Design+Patterns&ots=6YHotkX5yB&sig=gzJ2xIZEIa8rv5Mn-9gQynX6m\_0#v=onepage&q&f=false [Accessed 20 October 2021]

Phillips, D., Kasampalis, S. and Giridhar, C. (2016) *Python: Master the Art of Design Patterns*. Birmingham, UK: Packt Publishing. Available from: https://books.google.com/books?id=poNcDgAAQBAJ&pg=PA61&source=gbs\_toc\_r&cad=3#v=onepage&q&f=false [Accessed 18 October 2021]