Software engineering project

Requirements:

-The system should allow the user to register to the system using a username and password

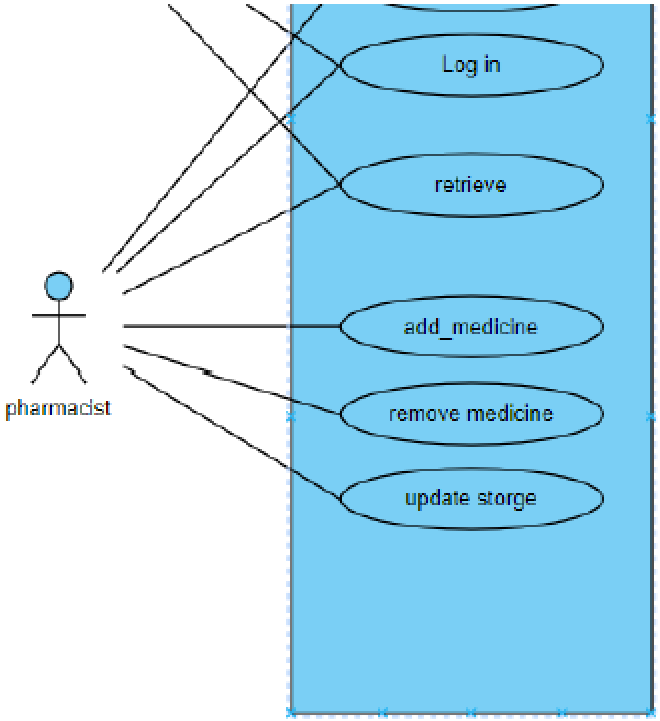
-The system should require the user to re-enter his username and password after 5-10 minutes of inactivity.

-The pharmacist can’t deny any entry he made to the medicines he has on the system.

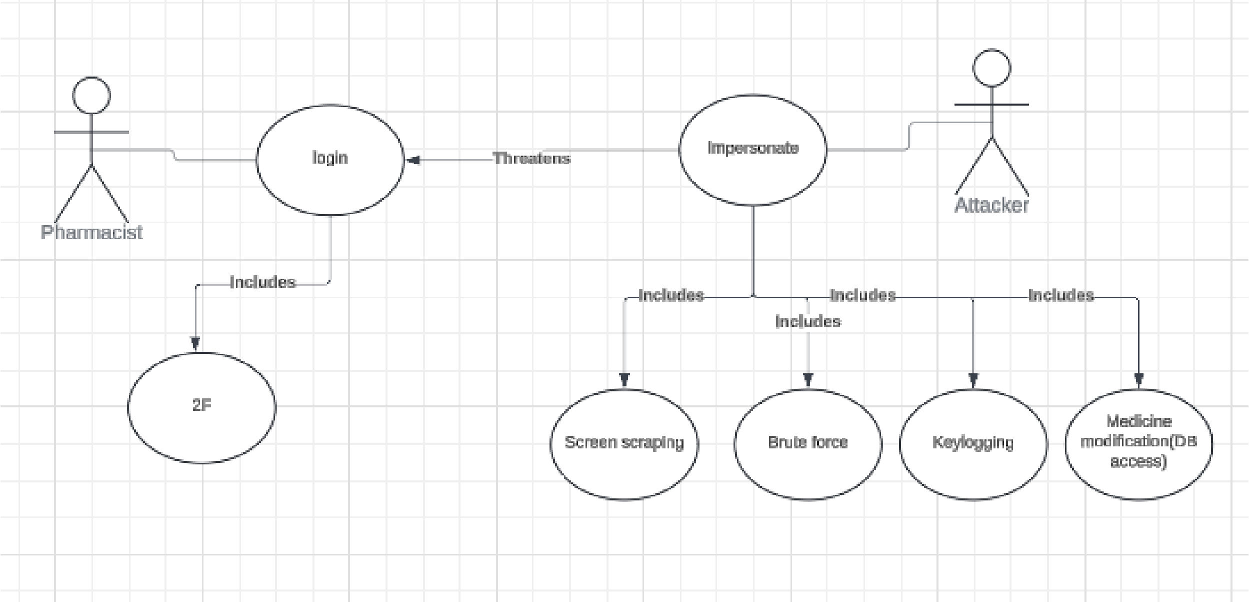
-The system should authenticate the users before accessing the system.

-Sensitive information should be hidden and encrypted in the database.

Use case:



Misuse case:



Misuse Case ID	L.1
Misuse case Name	screen scraping
Description	It's a malicious software that can capture screenshots of the desktop application while the user is entering their credentials to steal sensitive information
Preconditions	The attacker must install the malware to the application
postconditions	The attacker will have all the sensitive information that the pharmacist enters
Normal flow	1.The attacker finds a way to install the malware to the system 2. the attacker attempts to login to the system using the screenshots and the information he got
Mitigation	1.The workers in the hospital should be aware of any unnormal activity or suspicious people 2. Login attempts should be logged 3. A notification should be sent once a login happens to make sure who is the individual that logged in

Misuse Case ID	L.2
Misuse case Name	Using brute force to break into the system and use on of the pharmacist’s accounts
Description	The attacker will impersonate one of the pharmacists and use a brute forcing techniques to get the username and password
Preconditions	The attacker has access to the application
postconditions	The attacker can impersonate one of the pharmacists and login into the system
Normal flow	1.The attacker installs the application on a machine 2. The attacker uses a brute force technique to be able to login to the system using one of the pharmacist’s accounts
Mitigation	1.The system should have a lockout system where if a certain amount of unsuccessful logins occur the system will lock this account 2.Using strong password policy where the brute force attack will take a very long time to succeed 3. Sending an email to the actual pharmacist if a login happens to his account 4.Showing the date and time of the last login

Misuse Case ID	L.3
Misuse case Name	KeyLogging
Description	Using a malicious software to monitor every input entered by the users
Preconditions	Access to the application
postconditions	The attacker has all the information entered by the pharmacists
Normal flow	1.Attacker installs the malware on the application 2.Attacker uses the information that he gathers to log in to the system
Mitigation	1.Using antivirus or antimalware software 2.Being cautious with suspicious links or downloads 3.Using virtual keyboards while entering sensitive information 4.Monitor system activity

Misuse Case ID	L.4
Misuse case Name	Medicine Modification (DB access)
Description	After the attacker has access to one of the accounts he has the privilege to change the medicines available in the system
Preconditions	Attacker has to log in to the system successfully
postconditions	Attacker can modify the database and change the items as he wishes
Normal flow	1.Attacker uses one of the previous methods to enter the system 2.attacker has access to the database and can change the amount of the items or the availability of some of them
Mitigation	1.Implementing strong authentication and authorization controls 2.Using encrypted database where the attacker wont know the what the database has 3.Monitor the database activity 4.Secure backup and database recovery 5.Secure storage of the credentials