Software testing

Assignment2

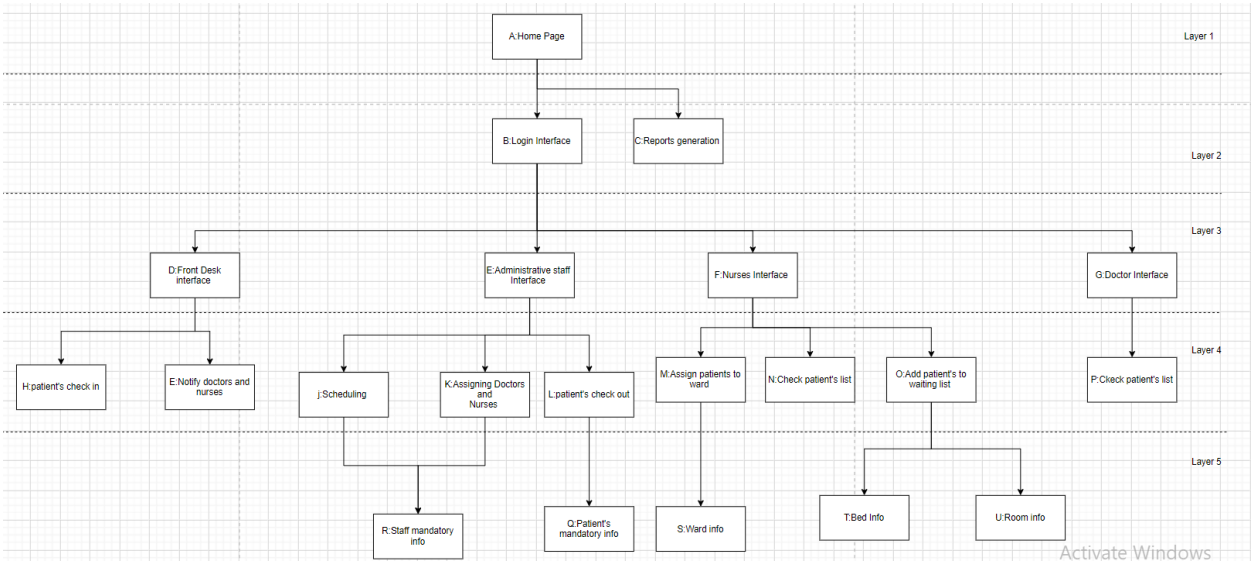
Name: Hana Yasser Amgad.

ID: 18p5007

Group: 2

Section: 2

1) Integration testing:



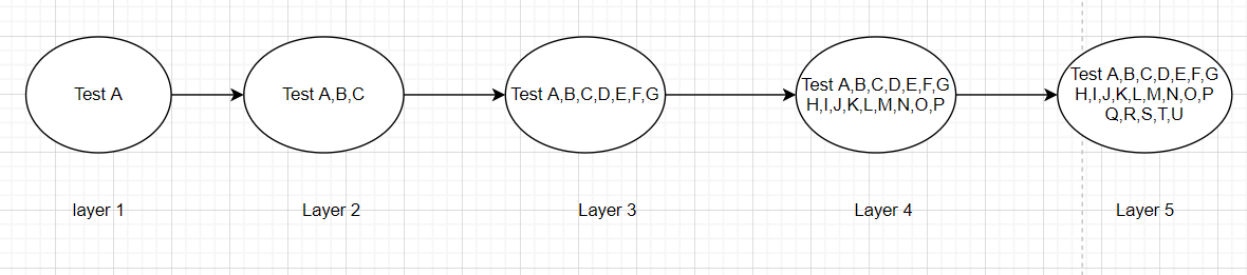
Assuming the system is composed of five layers, first the home page of the system. Second layer is the login in interface that based on the user (Front desk, Administrator, Nurse and Doctor), will lead him to the specified interface represented in the third layer, also consists of the functionality of generating reports that is dine automatically by the system. Fourth layer consist of functionalities that the systems offers to users, and last layer consists of all the data that should be retrieved by the user to accomplish his task.

Based on the implementation of the system and the flow of running and using it, a Top-down approach will be used to test it. Some stubs needed to compensate the unfished modules.

Test plan:

1. Test layer 1: open home page.
2. Test layer 1 and 2: open home page and login to work on the system.
3. Test layer 1, 2 and 3, ensuring that each user is led to the right interface.
4. Test layer 1, 2, 3 and 4: ensuring that each interface leads the user the operations that he is allowed to do on the system based on its accessibility (Stubs needed to compensate layer 4 as staff, patients and some other data are needed to complete the test of layer 3).
5. Now, all layers are implemented and the whole system can be tested.

Graphical representation of Top-down Test Technique:



2) System testing:
    1. Load testing:
        - Test that the system can handle up to 1000 people at a time.
        - Tests that the system can handle up to 600 registration per day.
        - Test that the system can generate up to 2000 reports per day.

    2. Limit testing:
        - Test that the system can support the maximum which is 1000 people at a time (system capacity), by checking on user interface response doesn't exceed 5 seconds and that system's response doesn't exceed 1 sec after checking patient's information.
        - Test the system can handle the maximum number of registrations per day (assuming 600 registration per day).
        - Test the system can handle generating the maximum number of reports (assuming 2000 reports per day), ensuring that there is no conflict in time as system should generate reports every six hours.

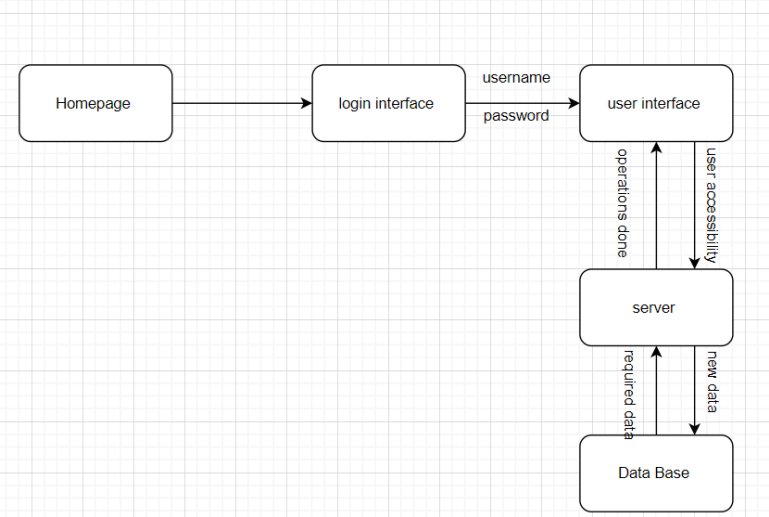
    3. Configuration testing:
        - Ensure that the system is compatible with windows 10.

    4. Soak testing:
        - Test system after a month of usage by checking on user interface response time and systems' response time after checking on data.

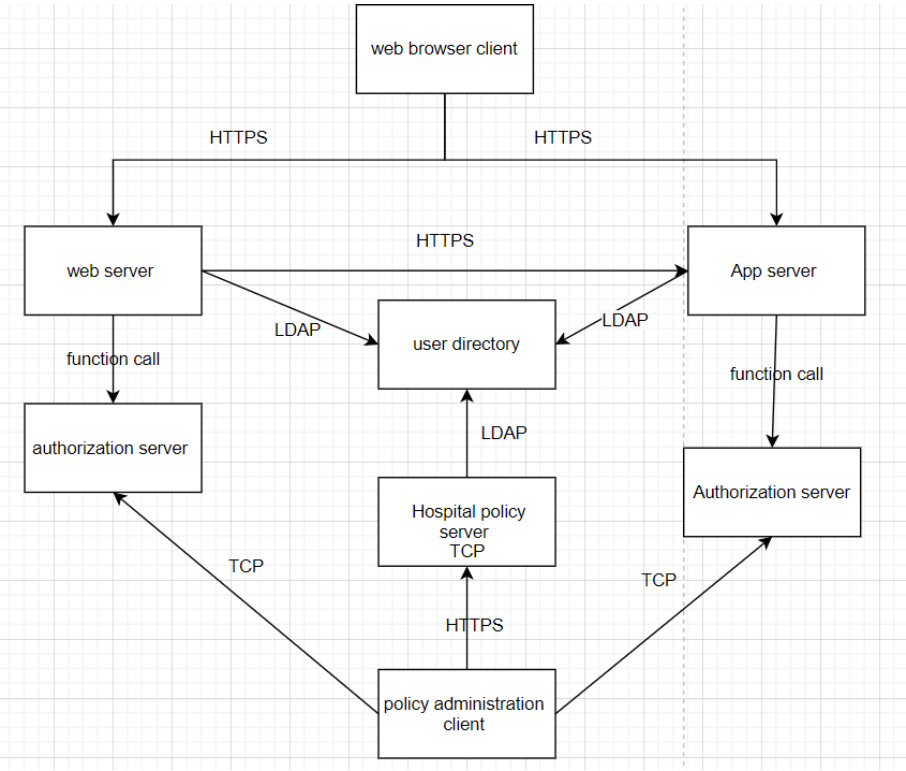
    5. Spike testing:
        - Test system's behavior while there is a sudden increment exceed in the load of concurrent users and registrations (ex: emergency cases).
        - Test system's behavior while 1 user is using it one day after an emergency case to test its behavior after a sudden decrement in load.
    6. Recovery testing:
        - Test system capability of retrieving data after s crash.
        - Test that if data is corrupted after a sudden shutdown.
    7. Security testing:
        - Penetration testing by trying to find if system contains bugs that threatens that system's security can be violated.

3) Security testing:

System is divided into components:



Security architecture:



Threat Modeling:

Assets:

1. Patients' data.
2. Medical staff data.
3. Credit card numbers.
4. Social security numbers.

Threats:

Spoofing identity (high):

System can be hacked by using fake identity where an administrator id and username can be stolen to get access to the system and steal any of the patient's data.

How to prevent this attack:

A timer can be used to determine at which time this user accessed system and send notification to the user on his private mail or mobile phone and also accessing hours can be saved on data base.

Denial of service (low):

System can deny responding to a normal order as adding or deleting some data, also it can be done in the form of refusing entry data format or even refusing admin accessibility.

How to prevent this attack:

A backup of data should be saved on a data base separate from the system in case any of the users faced this problem which will prevent loosing data or an operation failure, also system can trigger an error message to inform user that system denied his operation/ request and ask him to re-enter his id and password to re-do the operation.

Information disclosure (high):

This type of threat can be done if any of the users performed an operation that he doesn't have an accessibility on it. Ex: nurses access patient's data where they are not allowed to.

How to prevent this attack:

Ask user to scan his finger print/ID, to get access to data.

Tampering with data (medium):

A change in patients' or doctors' data or reports that cover patient's treatment plan can be done.

How to prevent this attack:

Making a back-up of data automatically 30 minutes after it entry and sending a notification comparing the official data to the new one.

Reduce the number of users that have access to data to minimize the possibility of changing data.

Threats ranking:

Spoofing identity (high):

A risk of having any another type of attacks that can be done by this hacker.

Affected people: Administrator staff.

Denial of service (low):

A big problem can occur as a consequences of the delay caused by the denial of the service.

Affected people: Admins, doctors, nurses and patients.

Information disclosure (high):

Data can be stolen.

Affected people: administrator staff.

Tampering with data (medium):

Change in Patients treatment plans and medical history.

Affected people: Admins, doctors, nurses and patients.