Republic of Iraq

Ministry of Higher Education

And Scientific Research

University of Technology

Computer Science Department

Information System Branch

Meassure the Security levels in Computer Network

A Project
Submitted to the department of computer science in the University of Technology in a partial fulfillment of the requirements for B.SC. Degree in computer science

By:

Mustafa Hussein Ali

Supervisor:

DR.Raheem Ogla

بسم الله الرحمن الرحيم

يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ
وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ
وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ

صدق الله العلي العظيم

Acknowledgements

Firstly all my prayers be to (Allah), the almighty, for the successive blessing divine providence, and my success in this thesis.

My greatest thanks are due to my supervisor **DR.Raheem Ogla**
for giving me the all opportunity and supporting me in this work, I would not have been able to finish this thesis without his guidance.

Special thanks are also due to head of **Computer Ssciences department of the University of Technology** and all the teaching staffs who have taught me.

Also, I wish to thank my friends for their help in good difficult times and for encouraging me to study and work.

Finally, u would like to thank my parents for their ongoing support and giving me assurance especially when I was really disappointed.

Mustafa Hussein Ali

Supervisor's Certification

I hereby certify that this project entitled ("**Meassure the Security Levels in Computer Network**") was prepared under my supervision at the Department of Computer Sciences of the University of Technology, as a partial fulfillment of the requirements for the B.Sc. Degree in Computer Sciences.

Signature:

Name:

Date:

Examination Committee Certificate

We certify that we have read this project ("**Meassure the Security Levels in Computer Network**"), and as an examining committee, examined the students ("hayder jabbar & bilal sattar ") in its content and what is related to it , and that in our opinion it meets the standard of a project for the degree of B.Sc. in Computer Sciences.

Signature:

Name:

Date :

Signature:

Name :

Date :

Chapter 1

1.1 What is Computer Security?

Computer security — a wide concept that encompasses almost any software or hardware that is designed to prevent the loss or theft of electronic data — is important for a number of reasons, but perhaps principally as a means of keeping information safe. Most of the time, the term “computer security” refers to the security of a computer’s insides. The data and compendious information that most users store on their hard drives is often far more valuable than are the machines themselves. Broadly speaking, the importance of computer security lies in how harmful it can be if that data is lost.

Most people think about computer security in a corporate or business context. Companies often store a lot of very sensitive information electronically, including trade secrets, customer lists and extensive corporate documents, both finished and those in progress.

1.2 Why is Computer Security Important?

The importance of computer security also extends to larger network security. A compromised computer can be manipulated and made into an agent of a cyber crime ring. Viruses and malware are often designed to hijack and exploit email address books, for instance.

1.3 What Does This Mean for Me?

- This means that everyone who uses a computer or mobile device needs to understand how to keep their computer, device and data secure.

>Information Technology Security is everyone's responsibility!

1.4Types of Computer Security

Computer security is one of the most important issues in organizations which cannot afford any kind of data loss.

Computer security is that branch of information technology which deals with the protection of data on a network or a stand-alone desktop. As every organization is dependent on computers, the technology of its security requires constant development. Here are the different types of computer security.

1.4.1 Hardware Security

Threat

Even if the computer is not plugged into a network, a person can open its cabinet and gain access to the hard drives, steal them and misuse or destroy the data saved on them or, damage the device altogether. It is also necessary to remember that in case one dissembles his computer hardware, the risk of losing coverage of warranty becomes very high.

Protection

The security of computer hardware and its components is also necessary for the overall protection of data. If a stand-alone system contains some important or classified information, it should be kept under constant surveillance. Locking system for a desktop and a security chain for a laptop are basic security devices for your machine.

1.4.2NetworkSecurity

Computer networks are an integral part of any organization these days, as they facilitate the free flow of data and services to the authorized users. However, such networks also pose a security threat in case the data is classified and confidential, thus making network securityavitalnecessity.

Threats

As the data is available only for authorized users, it is possible for hackers to pretend to be one, by providing the correct user name and password. Computer network security can be disrupted or encroachedinthefollowingways:

DenialofService:

Denial-of-service is meant to disable a computer or a network and can be executed with limited resources. It is one of the most common forms of attacks by hackers and can effectively disable the whole network of an organization.

TrojanHorse

Trojan horse is common and one of the most potential threats to computer security. They are malicious and security-breaking programs, disguised as something which is considered as non-malicious by the security software

Viruses and Worms

Viruses and worms are well-known for their destructive nature and

the property of replicating themselves. They are basically pieces of computer program codes, which are written by hackers and other computer geniuses.

Sniffing

Sniffing is the act of intercepting TCP/IP packets while they are getting transferred on a network. The interception generally takes place through simple eavesdropping done by a hacker.

Protection

Firewall

It is one of the most essential type of network security in today's world of Internet. Firewall is a filter that prevents fraud websites from accessing your computer and damaging the data. However, a firewall is not a great option for securing the servers on the Internet because the main objective of a server is granting access to unknown users to connect to various web pages.

Security Software

Along with firewall, try installing a good anti-virus and security software to enhance the security level of your computer system.

1.4.3 Data Security

Threat

Although uncommon, hardware malfunction can prove to be a major threat to your data in the computer. The life span of hard disks is always limited because of surrounding factors and this can amount to a severe loss of all your files saved on the disk, if there is no proper backup of those files made on any other system.

Protection

Keep Backup

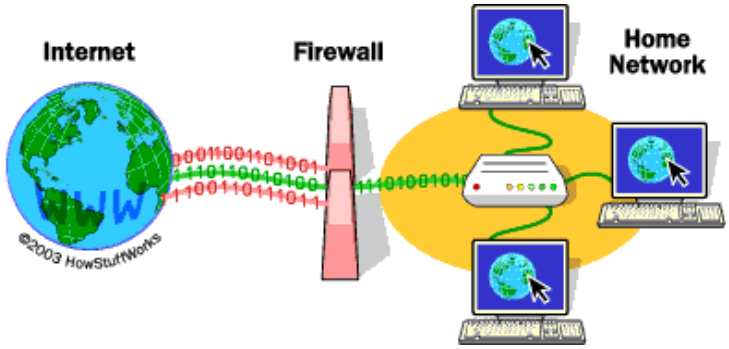
It is important to avoid data and information loss in case of hard disk crashes. The only solution is to regularly keep backups of all the data on other media such as magnetic tapes, CD-ROM, etc. It is a good practice to store the media off-site and in case of a disk crash, restore the information from the backup media onto the new disk

Clean-up Software

Install a software program on your computer that will clear all the old,

unused files and registry keys. It will also help to detect malware and save your computer from a severe damage caused by it. Keep your system in the loop of latest updates and security alerts or else, it will become vulnerable to security threats.

Chapter 2
Introdction to firewalls



2.1 What is a Firewall?

A firewall is a security device that can be a software program or a dedicated network appliance. *The main purpose of a firewall* is to separate a secure area from a less secure area and to control communications between the two. Firewalls can perform a variety of other functions, but are chiefly responsible for controlling inbound and outbound communications on anything from a single machine to an entire network.

2.1.1 Software Firewalls

Software firewalls, also sometimes called personal firewalls, are designed to run on a single computer. These are most commonly used on home or small office computers that have broadband access, which tend to be left on all the time. A software firewall prevents unwanted access to the computer over a network connection by identifying and preventing communication over risky ports.

2.1.2 Hardware Firewalls

Hardware firewalls are more complex. They also have software components, but run either on a specially engineered network appliance or on an optimized server dedicated to the task of running the firewall. The operating system underlying a hardware firewall is as basic as possible and very difficult to attack. Since no other software runs on these machines, and configuration takes a little more thought than clicking on an "allow" prompt, they are difficult to compromise and tend to be extremely secure.

Firewalls are also used for Network Address Translation (NAT). This allows a network to use private IP addresses that are not routed over the Internet. Private IP address schemes allow organizations (or even household networks) to limit the number of publicly routed IP addresses they use, reserving public addresses for Web servers and other externally accessed network equipment.

2.2 the different types of Firewall technologies

there is three common types of firewalls are:

1.Packet Filtering Firewalls
2. Circuit level gateway Firewalls
3. Application level gateway Firewalls

2.2.1 Packet Filtering Firewalls:

Packet Filtering mechanisms work in the network layer of the OSI model. In packet filtering, each packet passing through a firewall is compared to a set of rules before it is allowed to pass through. Depending on the packet and the rule, the packet can be either dropped, sent through or a message can be forwarded to the originator.

2.2.2 Circuit level gateway Firewalls:

The circuit level gateway firewalls work at the session layer of the OSI model. They monitor TCP handshaking between the packets to determine if a requested session is legitimate. And the information passed through a circuit level gateway, to the internet, appears to have come from the circuit level gateway.

2.2.3 Application level gateway Firewalls:

Application level firewalls decide whether to drop a packet or send them through based on the application information (available in the packet). They do this by setting up various proxies on a single firewall for different applications. Both the client and the server connect to these proxies instead of connecting directly to each other. So, any suspicious data or connections are dropped by these proxies.

2.3 Firewalls advantages

It is very important to know that the firewall is one of the most effective forms of protection developed against the hackers operating on the Internet , Firewalls use a variety of techniques to protect against the attacks such as proxy servers .

You have to know that the firewall controls the network access to one or more computers , The Internet is a large network that includes your computer , The firewall protects your computer by acting as a gate through which both all the data must pass , It blocks certain kinds of traffic .

2.4 Disadvantage of firewalls

It is very important to know that a dedicated hardware firewall costs more than a software firewall , It is difficult to install , and upgrade , It takes up physical space , and involves wiring .

You should know that the hardware firewalls tend to be more expensive than the software firewalls , When the hardware firewalls can not run on the computer, they can be a challenging to configure .

Chapter 3
Network Critiria

3.1 **Performance Efficiency or performance**

It is possible to know the efficiency or performance in many ways, but now performance depends on the time of transition and response time, and we can define the time of the transition Transit Time on that amount of time required for the transmission of data in order to pass or move from one element to another element

The Response Time Response time is the time that goes on between the Send demand and get the biggest response from the time of the transition, and we can calculate the response time of the equation or the following law.

Response Time = 2 * Transit Time + Processing Time

3.1.1 users number

Each calculator on the network is the user, and the number of users affects the response time and everything has increased the number of users will decrease the performance of the network because the response time will increase, while the transition time will remain constant because the distance between the remaining computers be fixed …

3.1.2 The quality of the center carrier

Nature of the material carrier data affect the process of the transfer (data) transfer rate between devices...

3.1.3 Materialism

Materialism will affect the speed and the amount of the amount of storage whether the sender or recipient or the contract moderation Node

3.1.4 Software

Programmatic entity is used in both the sender and the recipient, or the recipient of moderation and the contract, and everything was faster processing software and implementation greater the efficiency of the network.

3.2 Reliability

Any network where the number a few times where the reliability of failure is high it be any inverse relationship.

3.3 Security

If the network security with high performance or have highly efficient especially if they specialized in one of the areas of data protection and are in two areas:

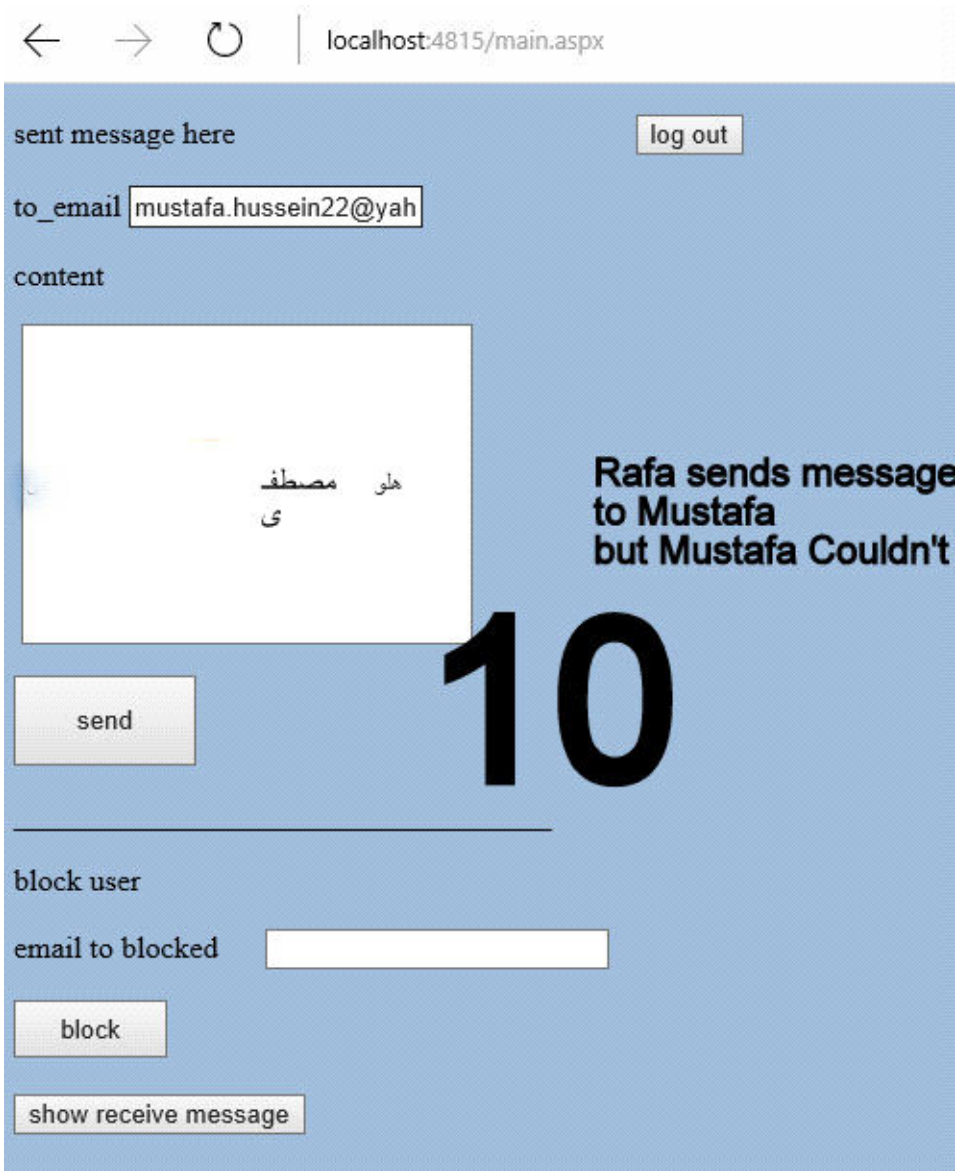
3.3.1 unauthorized access

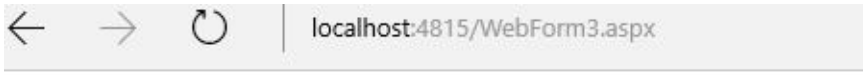
In the network are no public data and private data are public data from the user right to see it, but the data are not entitled to the user to view them as they are with high security and access to it is not authorized to do.

3.3.1 viruses

There are several types of viruses on the network you delete the data on the computer.

my program writed with asp.n


localhost:4815/main.aspx
sent message here
log out
to_email
mustafa.hussein22@yah
content
هلو مصطفى
Rafa sends message
to Mustafa
but Mustafa Couldn't
10
send
block user
email to blocked
block
show receive message

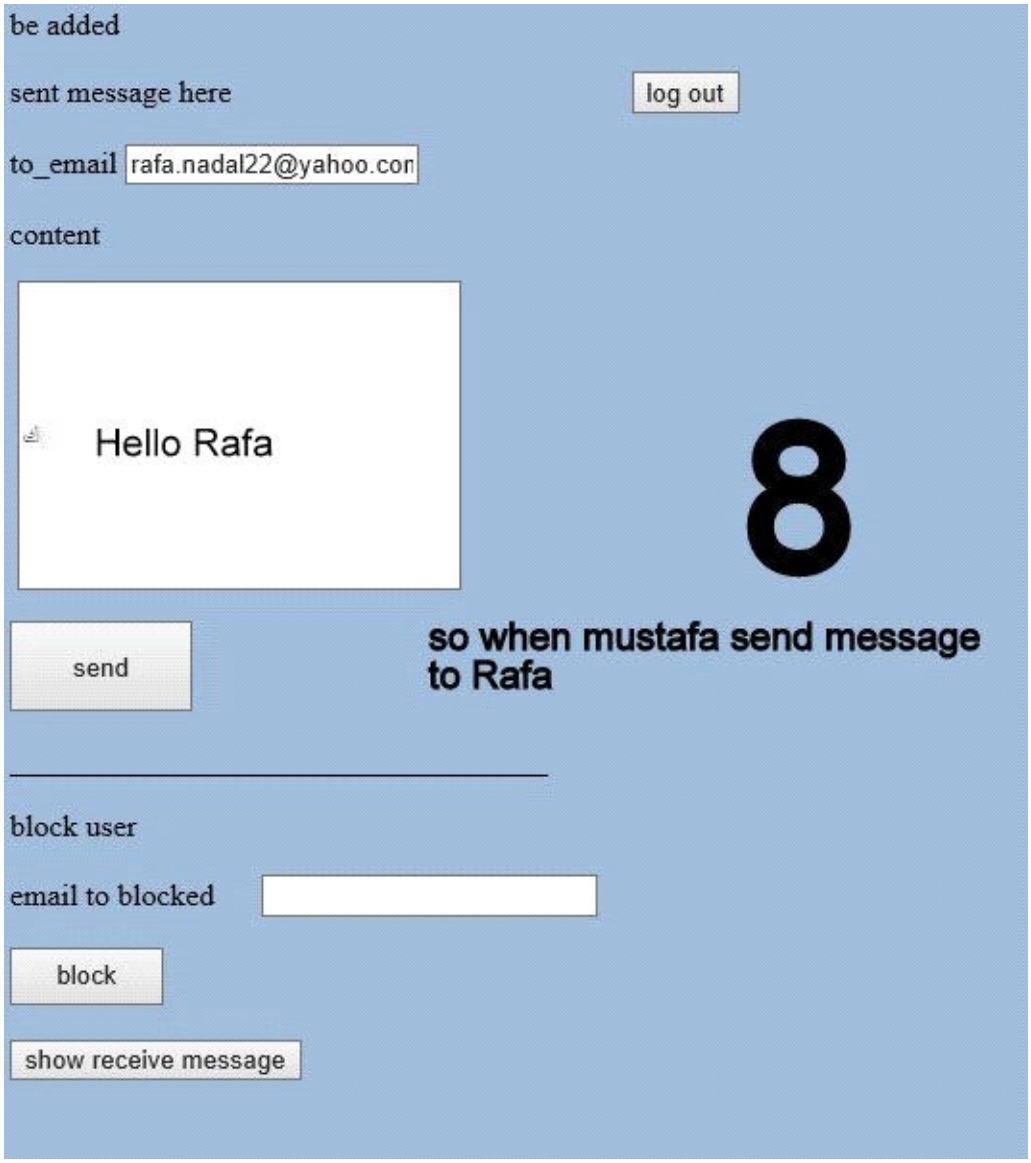


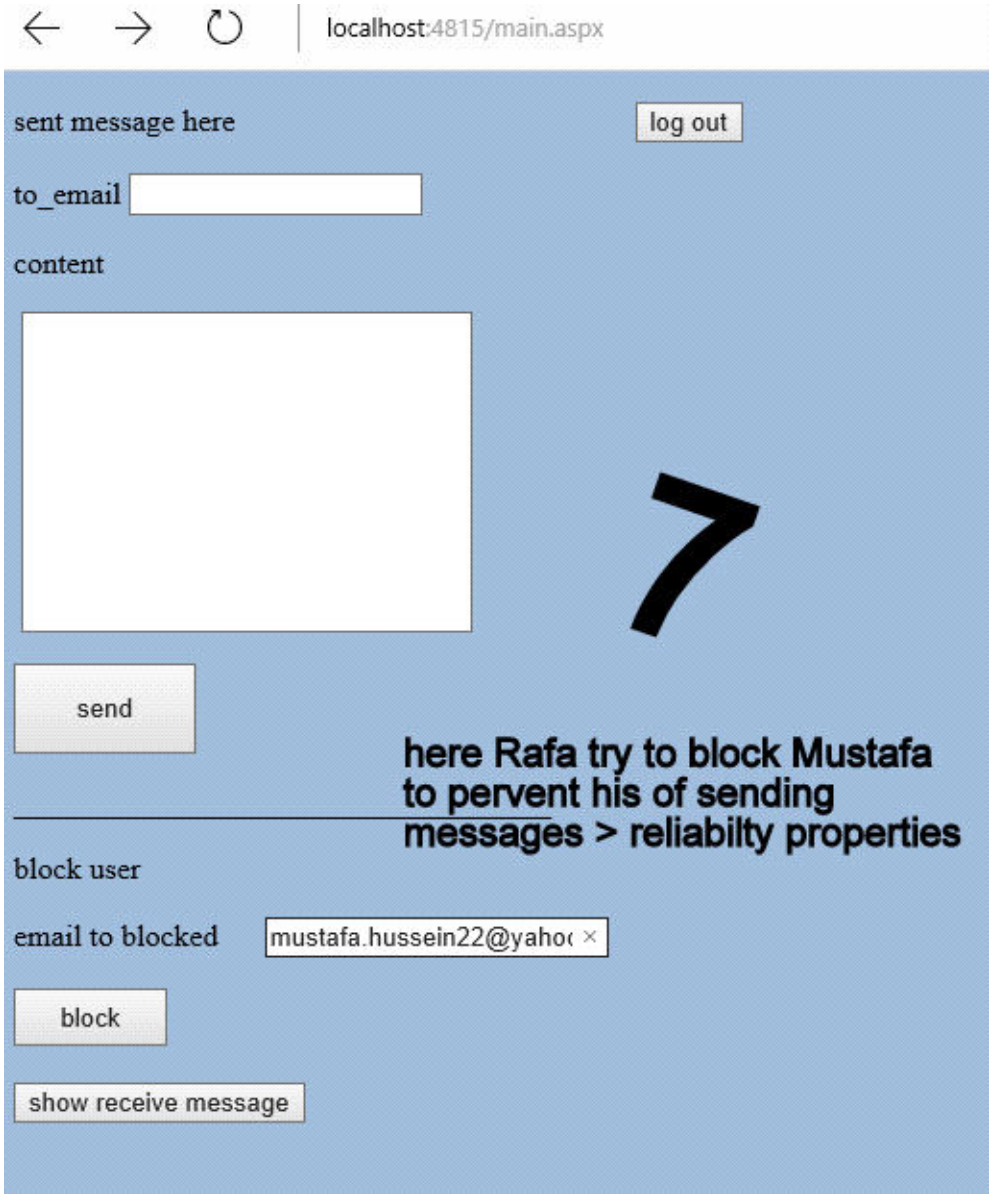
9

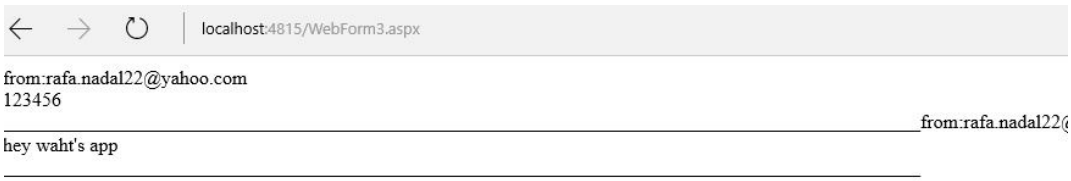
there is no message from Mustafa
so he's blocked

but

Rafa still has the ability of sending messages
to Mustafa

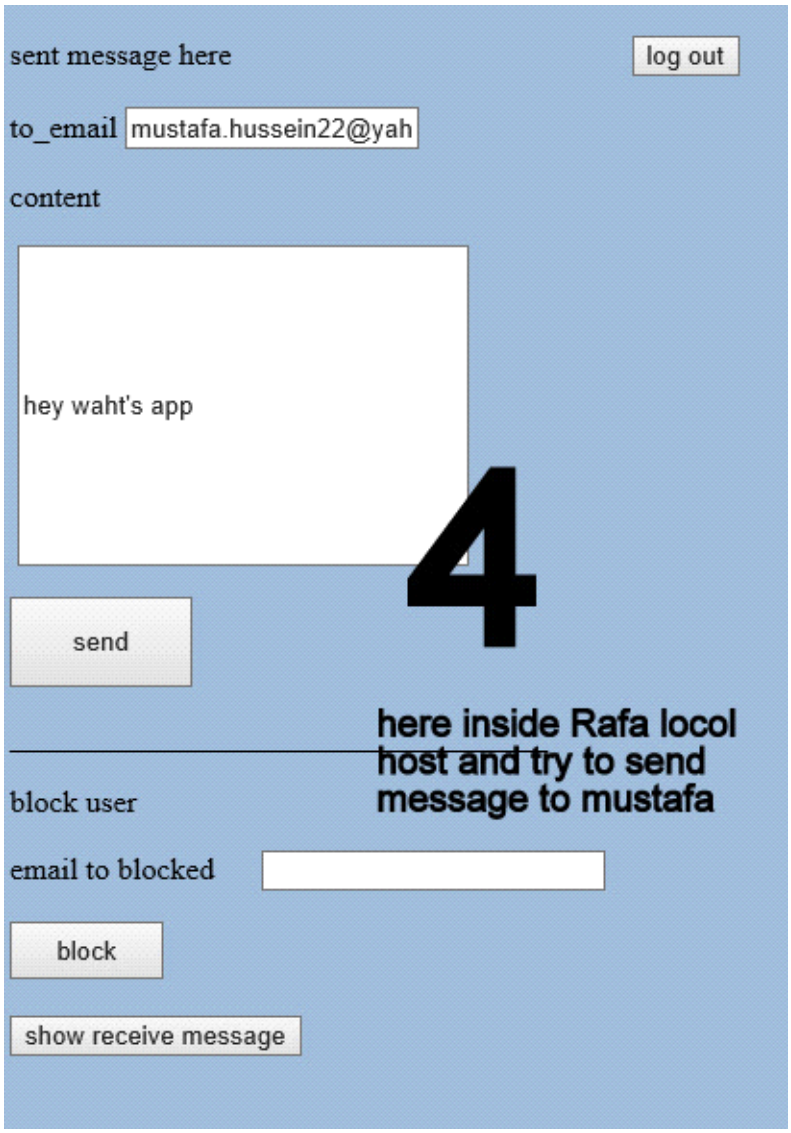

be added
sent message here
log out
to_email
rafa.nadal22@yahoo.con
content
Hello Rafa
8
send
so when mustafa send message to Rafa
block user
email to blocked
block
show receive message

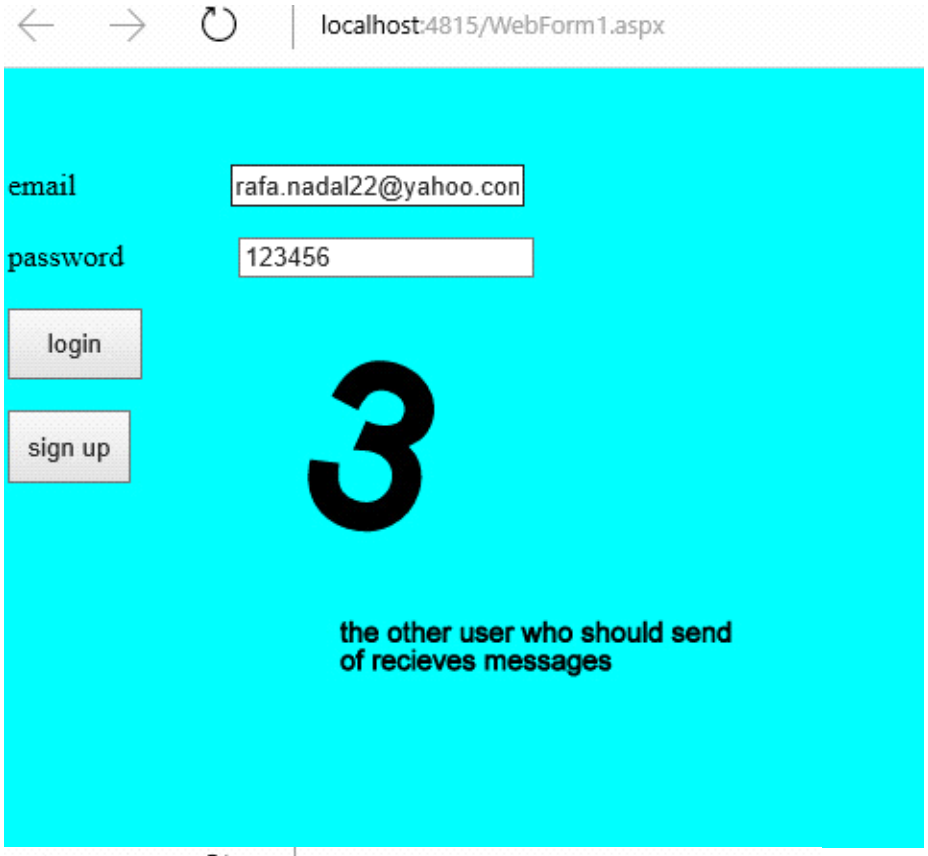

localhost:4815/main.aspx
sent message here
log out
to_email
content
7
send
here Rafa try to block Mustafa
to pervent his of sending
messages > reliabilty properties
block user
email to blocked
mustafa.hussein22@yaho
block
show receive message

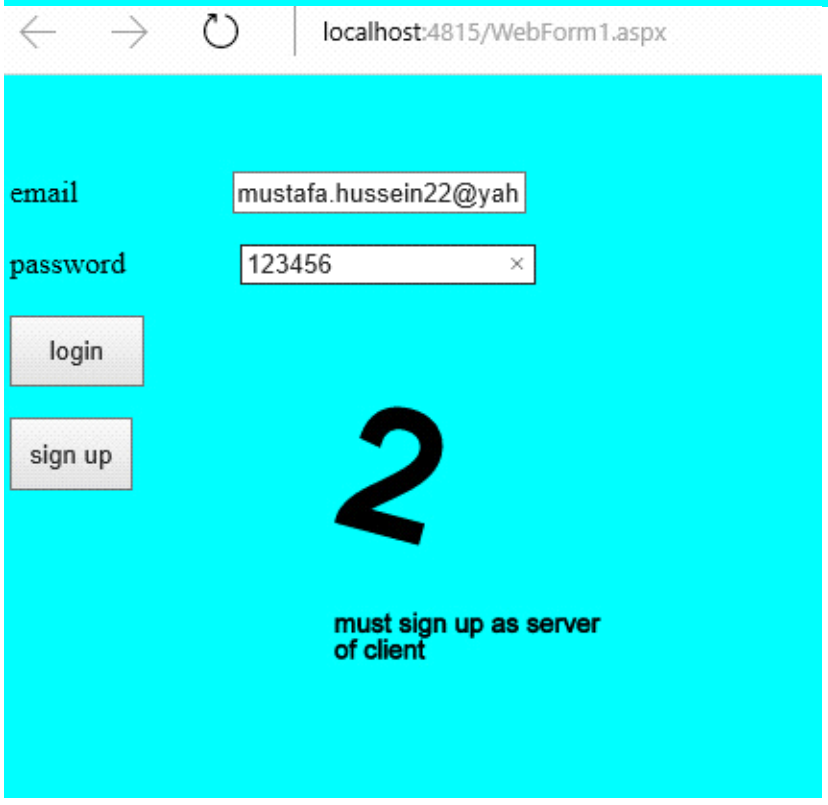


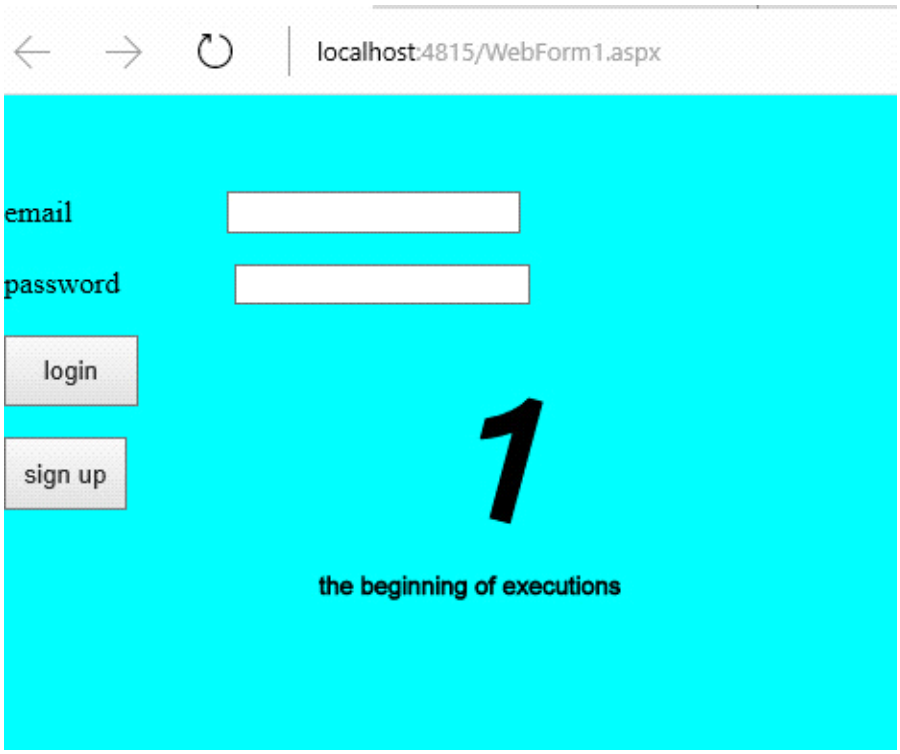
5

when mustafa open his account
he found this message from Rafa


sent message here
log out
to_email
mustafa.hussein22@yah
content
hey waht's app
4
send
here inside Rafa locol host and try to send message to mustafa
block user
email to blocked
block
show receive message


localhost:4815/WebForm1.aspx
email
rafa.nadal22@yahoo.con
password
123456
login
sign up
3
the other user who should send
of recieves messages


localhost:4815/WebForm1.aspx
email
mustafa.hussein22@yah
password
123456
login
sign up
2
must sign up as server
of client



Refrences

Network security, lesson 2: Common security measur e

http://searchitchannel.techtarget.com/feature/Whatare thecriteriaforsuccessfulnetworkperformance-management

network security of computer jack isner book.

http://www.windowstalk.org/3typesofcomputer-security/

Robin Snader Department of Computer Science
University of Illinois at Urbana–Champaign
rsnader2@cs.uiuc.edu