The first very obvious vulnerability is that the chat can be interrupted by the third party and if accidently accepted, will cause target redirected to the third person. To prevent this, we can set the server side stop listening after one chat started. After current chat end, start listen again with same port.

Another vulnerability is that this app does not have reliable transmission. The packet could get lost. To solve this, just let the program send an ack back for every received packet, if it cannot get ack, resend the packet.

Except that the chat could be interrupted by a bogus message, it can also be terminated by that message. Someone could fake the IP and send message to one of the peers.