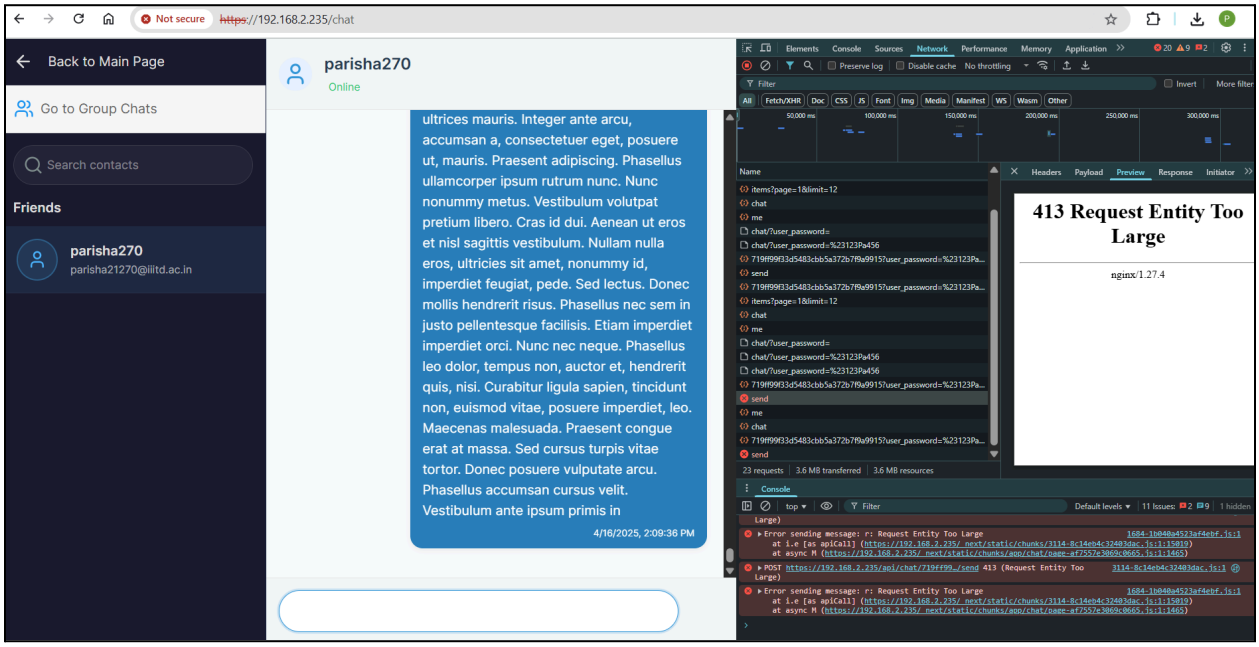
Group no: 3

Vulnerability Type:
Security

Brief Discription: There is no restriction on the size of the messages sent by the users so i can send a very large message and cause the server to slow down a lot and possibly crash as well. As the backend is not handling oversized payloads it can potentially result in DOS attack vulnerable.

Steps to Reproduce:
1) Go to https://192.168.2.235/chat
2) Select any user to chat with and send very large msg (like 100000 words)
3) Then see that the site slows down a lot and gives errors.

Proof of Concept:
I have send a very large messages of approx 100000 words. As there is no limit on msg length, i can significantly slow down the server and possibly crash it as well. We can see here that the send button had also disappeared and the website was becoming unresponsive.



Impact:
As there is no message size restrictions and no proper input validation this makes the sitevulnerable to Denial of Service (DoS) attacks. Also attackers can crash or hang the server by sending large messages repeatedly. Could lead to database bloating, performance degradation, and site downtime. If error traces or logs are exposed, it may also lead to information leakage and further exploitation