Group no: 14

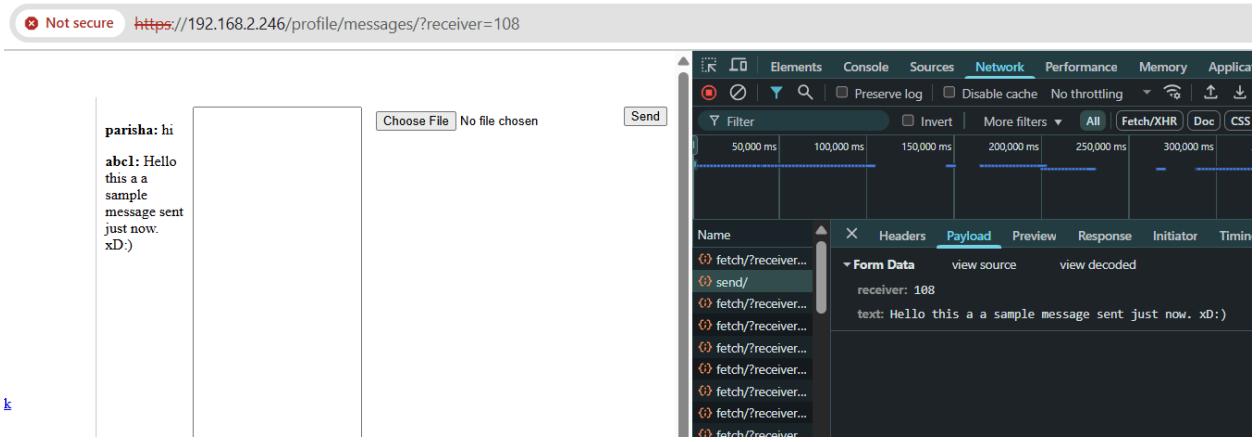
Vulnerability Type:
Security (and bit functional as well)

Brief Discription: In this there is no true e to e encryption in the messaging flow as messages are being sent as plaintext which exposes sensitive information to anyone with access to the network traffic like through a proxy or mitm attack. This could result in a breach of user confidentiality and data integrity.

Steps to Reproduce:

1) Go to https://192.168.2.246/profile/messages/?receiver=108
2) Send any message to the user.
3) Go to the network tab in inspect elements (ctrl+shift+i).
4) See the network activity during the message transmission i.e the endpoint https://192.168.2.246/profile/messages/send/.
5) Click on the send endpoint and in the payload section see that this post request to the send/ endpoint has the message content in plaintext.

Proof of Concept:
I sent a message: Hello this a a sample message sent just now. xD:) to the username parisha. I saw that the POST request to: https://192.168.2.246/profile/messages/send/ has the plaintext form data and there is no encryption or obfuscation to user messages in transit which makes these vulnerable to interception.



Impact:
This bug exposes all user messages to a network sniffing &interception attacks especially in non-secure environments like public Wi-Fi as any attacker on the same network can easily read, log or manipulate private messages. This breaks confidentiality and may lead to serious privacy violations and data leaks.