Group no: 14

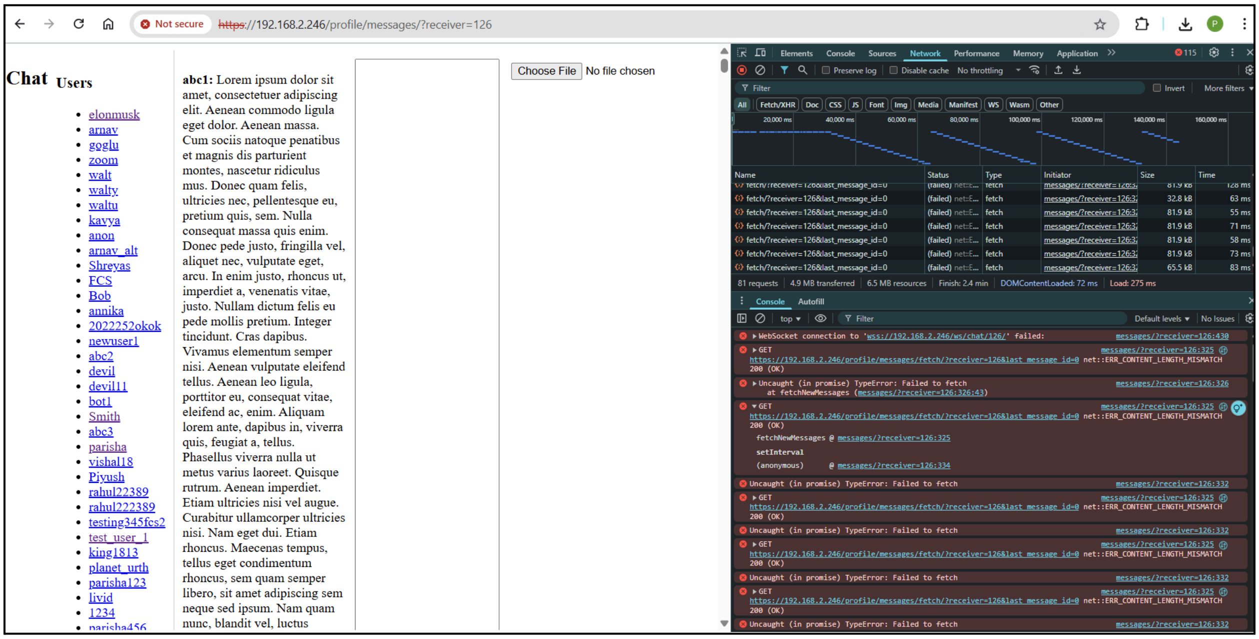
Vulnerability Type:
Security

Brief Discription: There no limit on length check in messages. So i can send vey large message (>10000 words) so that as system attempts to process and render the data it uses significant resources and I can also thus fill the server database as well with large msgs to cause DOS attack vulnerablility.

Steps to Reproduce:

1) Go to https://192.168.2.246/profile/messages/
2) Select any user to chat with and sens a very large msg (like 10000 words)
3) Then in the inspect tab (ctrl+sft+i) we can see the failed WebSocket communication and repeated fetch calls to profile/messages/fetch/?receiver=126.

Proof of Concept:
I have send multiple large messages of approx 10000 words each. As there is no limit on msg length, i can see that the web socket is failing anf the site is becoming slow with periodic fetch failures every few seconds.



Not secure ~~https~~://192.168.2.246/profile/messages/?receiver=126

Chat Users

- elonmusk
- arnav
- goglu
- zoom
- walt
- walty
- waltu
- kavya
- anon
- arnav_alt
- Shreyas
- FCS
- Bob
- annika
- 2022252okok
- newuser1
- abc2
- devil
- devil11
- bot1
- Smith
- abc3
- parisha
- vishal18
- Piyush
- rahul22389
- rahul222389
- testing345fcs2
- test_user_1
- king1813
- planet_urth
- parisha123
- livid
- 1234
- parisha456

abc1: Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo, rhoncus ut, imperdiet a, venenatis vitae, justo. Nullam dictum felis eu pede mollis pretium. Integer tincidunt. Cras dapibus. Vivamus elementum semper nisi. Aenean vulputate eleifend tellus. Aenean leo ligula, porttitor eu, consequat vitae, eleifend ac, enim. Aliquam lorem ante, dapibus in, viverra quis, feugiat a, tellus. Phasellus viverra nulla ut metus varius laoreet. Quisque rutrum. Aenean imperdiet. Etiam ultricies nisi vel augue. Curabitur ullamcorper ultricies nisi. Nam eget dui. Etiam rhoncus. Maecenas tempus, tellus eget condimentum rhoncus, sem quam semper libero, sit amet adipiscing sem neque sed ipsum. Nam quam nunc, blandit vel, luctus

Choose File No file chosen

Name	Status	Type	Initiator	Size	Time
fetch/?receiver=126&last_message_id=0	(failed) net::E...	fetch	messages/?receiver=126:3	81.9 kB	128 ms
fetch/?receiver=126&last_message_id=0	(failed) net::E...	fetch	messages/?receiver=126:3	32.8 kB	63 ms
fetch/?receiver=126&last_message_id=0	(failed) net::E...	fetch	messages/?receiver=126:3	81.9 kB	55 ms
fetch/?receiver=126&last_message_id=0	(failed) net::E...	fetch	messages/?receiver=126:3	81.9 kB	71 ms
fetch/?receiver=126&last_message_id=0	(failed) net::E...	fetch	messages/?receiver=126:3	81.9 kB	58 ms
fetch/?receiver=126&last_message_id=0	(failed) net::E...	fetch	messages/?receiver=126:3	81.9 kB	73 ms
fetch/?receiver=126&last_message_id=0	(failed) net::E...	fetch	messages/?receiver=126:3	65.5 kB	83 ms

81 requests | 4.9 MB transferred | 6.5 MB resources | Finish: 2.4 min | DOMContentLoaded: 72 ms | Load: 275 ms

```
▶WebSocket connection to 'wss://192.168.2.246/ws/chat/126/' failed:        messages/?receiver=126:430
▶GET                                                                        messages/?receiver=126:325
https://192.168.2.246/profile/messages/fetch/?receiver=126&last_message_id=0 net::ERR_CONTENT_LENGTH_MISMATCH
200 (OK)
▶Uncaught (in promise) TypeError: Failed to fetch                          messages/?receiver=126:326
    at fetchNewMessages (messages/?receiver=126:326:43)
▼GET                                                                        messages/?receiver=126:325
https://192.168.2.246/profile/messages/fetch/?receiver=126&last_message_id=0 net::ERR_CONTENT_LENGTH_MISMATCH
200 (OK)
  fetchNewMessages @ messages/?receiver=126:325
  setInterval
  (anonymous)      @ messages/?receiver=126:334
Uncaught (in promise) TypeError: Failed to fetch                           messages/?receiver=126:332
▶GET                                                                        messages/?receiver=126:325
https://192.168.2.246/profile/messages/fetch/?receiver=126&last_message_id=0 net::ERR_CONTENT_LENGTH_MISMATCH
200 (OK)
Uncaught (in promise) TypeError: Failed to fetch                           messages/?receiver=126:332
▶GET                                                                        messages/?receiver=126:325
https://192.168.2.246/profile/messages/fetch/?receiver=126&last_message_id=0 net::ERR_CONTENT_LENGTH_MISMATCH
200 (OK)
Uncaught (in promise) TypeError: Failed to fetch                           messages/?receiver=126:332
▶GET                                                                        messages/?receiver=126:325
https://192.168.2.246/profile/messages/fetch/?receiver=126&last_message_id=0 net::ERR_CONTENT_LENGTH_MISMATCH
200 (OK)
Uncaught (in promise) TypeError: Failed to fetch                           messages/?receiver=126:332
```

Impact:
I can repeatedly send large messages and can crash or hang the server/client by filling up the database and thus disrupting service for others thus causing a Denial of Service (DoS) attack. As there is no input sanitization or message size limit the site is vulnerable to abuse and performance degradation.