Group no: 5

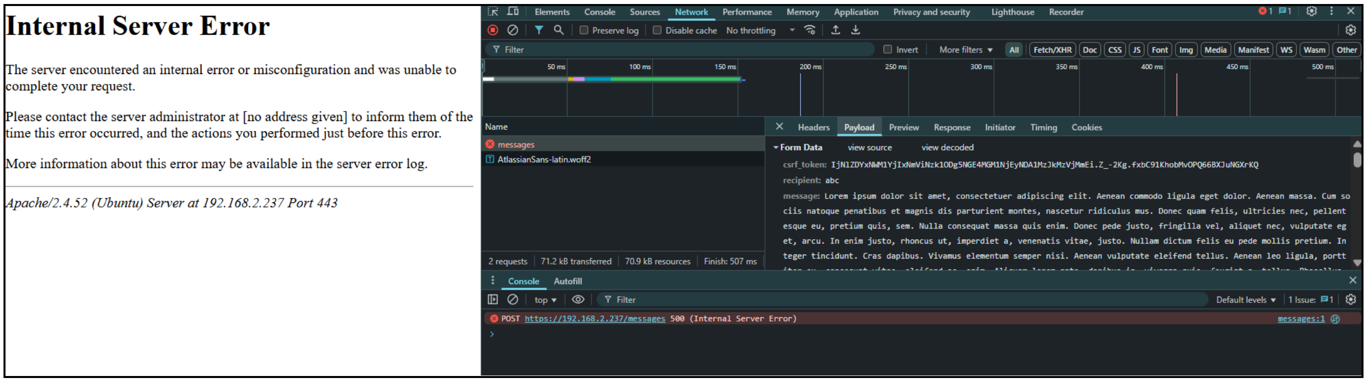
Vulnerability Type:
Security

Brief Discription: The site does not restrict the size of the messages sent by the users so i can send a very large message and cause the server to crash and return an HTTP 500 Internal Server Error. So backend is not handling oversized payloads and lacks proper input validation which can potentially result in DOS attack vulnerable.

Steps to Reproduce:

1) Go to https://192.168.2.237/messages
2) Select any user to chat with and send very large msg (like 100000 words)
3) Then see that the site throws a 500 Internal Server Error response.
4) Now the site is down as its crashed and the server is unresponsive.

Proof of Concept:
I have send a very large messages of approx 100000 words. As there is no limit on msg length, i can crash the server as well for some time.



Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator at [no address given] to inform them of the time this error occurred, and the actions you performed just before this error.

More information about this error may be available in the server error log.

Apache/2.4.52 (Ubuntu) Server at 192.168.2.237 Port 443

Form Data

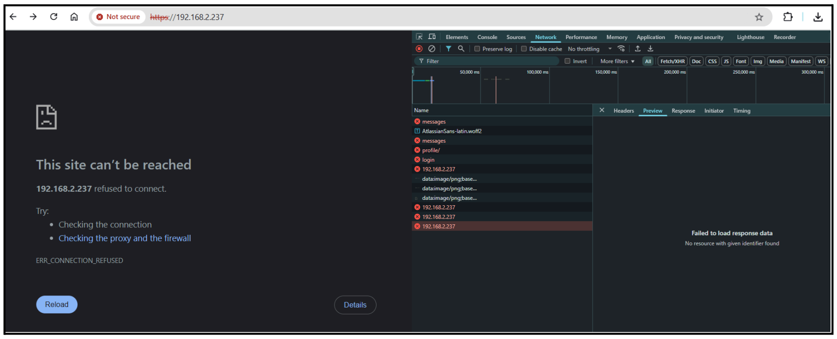
csrf_token: IjN1ZDYxNWM1YjIxNmViNzk1ODg5NGE4MGM1NjEyNDA1MzJkMzVjMmEi.Z_-2Kg.fxbC91KhobMvOPQ66BXJuNGXrKQ

recipient: abc

message: 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, portt

2 requests | 71.2 kB transferred | 70.9 kB resources | Finish: 507 ms

```
POST https://192.168.2.237/messages 500 (Internal Server Error)          messages:1
```



Not secure ~~https~~://192.168.2.237

This site can't be reached

192.168.2.237 refused to connect.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

Name
messages
AtlassianSans-latin.woff2
messages
profile/
login
192.168.2.237
data:image/png;base...
data:image/png;base...
data:image/png;base...
192.168.2.237
192.168.2.237
192.168.2.237

Failed to load response data
No resource with given identifier found

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. It can also cause to fill up the database and performance degradation thus site downtime.