Group no: 14

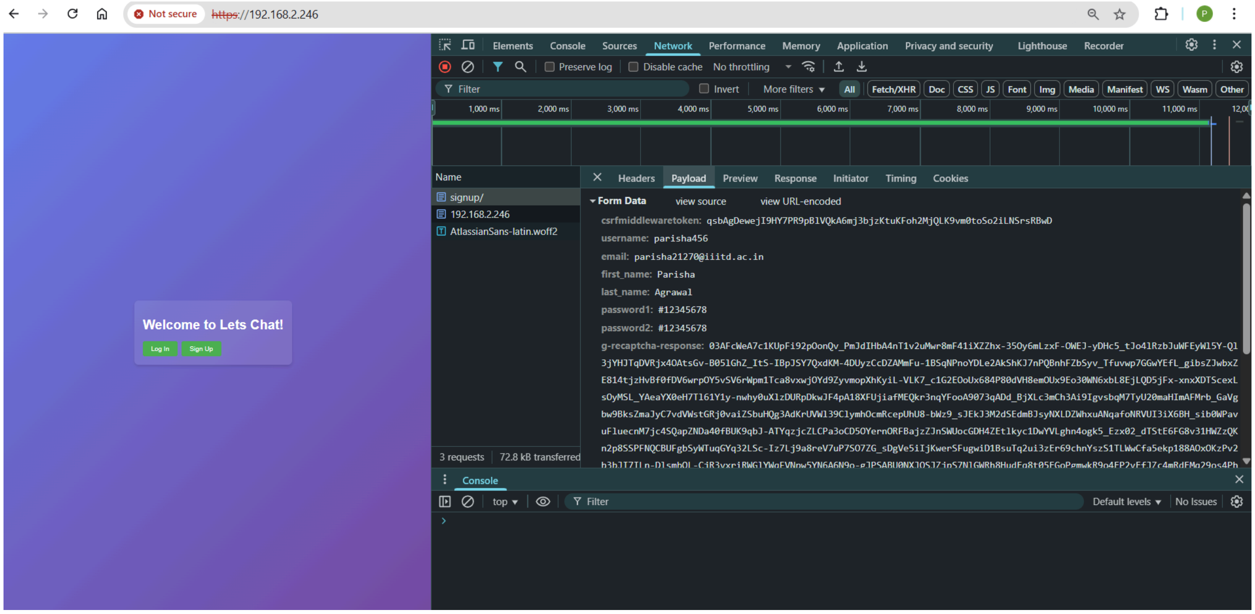
Vulnerability Type:
Functional (with security concern as well)

Description: The site transmits sensitive user data like passwords and email addresses as raw data without securing.

Steps to Reproduce:

1) Go to https://192.168.2.246.
2) Signup for new account or login to a existing one.
3) After signup or login, see the payload in the api, it has the raw password stored in it without encryption.

Proof of Concept:
Here we can see the raw password as well which violated requirement of secure data.



```
csrfmiddlewaretoken: qsbAgDewejI9HY7PR9pBlVQkA6mj3bjzKtuKFoh2MjQLK9vm0toSo2iLNSrsRBwD
username: parisha456
email: parisha21270@iiitd.ac.in
first_name: Parisha
last_name: Agrawal
password1: #12345678
password2: #12345678
g-recaptcha-response: 03AFcWeA7c1KUpFi92pOonQv_PmJdIHbA4nT1v2uMwr8mF41iXZZhx-35Oy6mLzxF-OWEJ-yDHc5_tJo41RzbJuWFEyWl5Y-Ql
3jYHJTqDVRjx4OAtsGv-B05lGhZ_ItS-IBpJSY7QxdKM-4DUyzCcDZAMmFu-1BSqNPnoYDLe2AkShKJ7nPQBnhFZbSyv_Tfuvwp7GGwYEfL_gibsZJwbxZ
E814tjzHvBf0fDV6wrpOY5vSV6rWpm1Tca8vxwjOYd9ZyvmopXhKyiL-VLK7_c1G2EOoUx684P80dVH8emOUx9Eo30WN6xbL8EjLQD5jFx-xnxXDTScexL
sOyMSL_YAeaYX0eH7Tl61Y1y-nwhy0uXlzDURpDkwJF4pA18XFUjiafMEQkr3nqYFooA9073qADd_BjXLc3mCh3Ai9IgvsbqM7TyU20maHImAFMrb_GaVg
bw9BksZmaJyC7vdVWstGRj0vaiZSbuHQg3AdKrUVWl39ClymhOcmRcepUhU8-bWz9_sJEkJ3M2dSEdmBJsyNXLDZWhxuANqafoNRVUI3iX6BH_sib0WPav
uFluecnM7jc4SQapZNDa40fBUK9qbJ-ATYqzjcZLCPa3oCD5OYernORFBajzZJnSWUocGDH4ZEtlkyc1DwYVLghn4ogk5_Ezx02_dTStE6FG8v31HWZzQK
n2p8SSPFNQCBUFgbSyWTuqGYq32LSc-Iz7Lj9a8reV7uP7SO7ZG_sDgVe5iIjKwerSFugwiD1BsuTq2ui3zEr69chnYszS1TLWwCfa5ekp188AOxOKzPv2
b3bJI7ILn-DlsmbOL-CjR3vxriBWGlYWgFVNpw5YN6A6N9o-gJPSABU0NXJOSJZjpS7NlGWRh8HudFq8t05EGoPgmwkR9o4FP2vEfJ7c4mRdFMg29os4Ph
```

Impact:
This violates the requirement in the course project requirement document that personal user data must be protected and using HTTPS(TLS/SSL) to secure data in transit. It can aslo couse credential theft through MITM attacks on open or local networks.