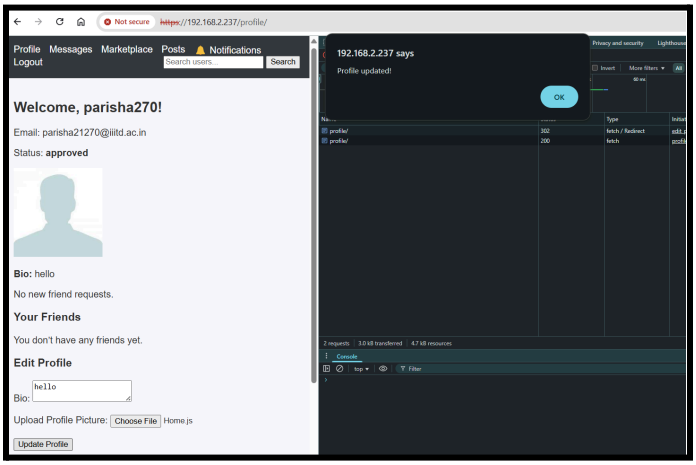
Group no: 5

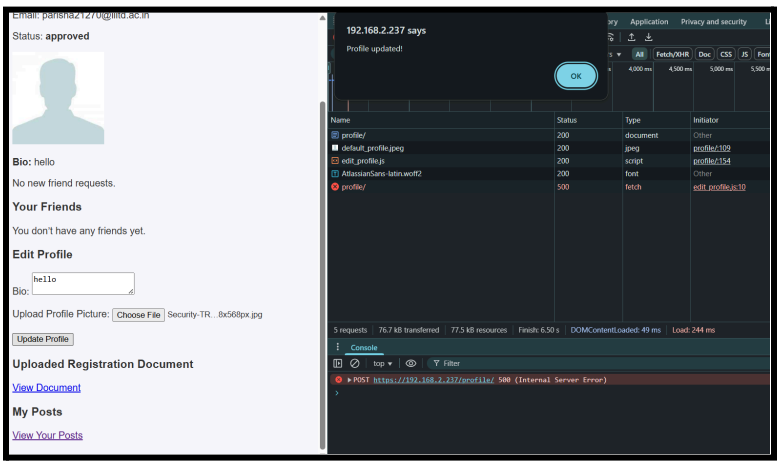
Vulnerability Type:
Functional (with bit security concern also)

Description: In the project requirement document, it was required that users can update username, profile picture in Profile Management. But in the ui there is no option to update the username and we can only update the bio and profile picture. Also in upload profile picture it accepts invalid files with .html or .js format which is dangerous and when I upload a valid file with .jpg profile picture the image does not appear on the profile page.

Steps to Reproduce:
1) Go to the url: https://192.168.2.237
2) Login with any existing account or with a new account.
3) There is no option to update username.
4) Then upload a .jpg image for profile picture.
5) We get the success message Profile updated but still the image does not update on the profile.
6) Then upload files like .html or .js as profile pictures. You will se e that it accepts these without validation.

Proof of Concept:
I uploaded a js file and no error was given and i got "Profile updated" successfully. Also when i uploaded a .jpg file, i the image is not updated.





Impact:
This violates the profile management requirements as users can't update their username. Also profile picture uploads do not work as expected which misleads the users and degrade the trust. There is security issue as well as profile picture accepts .js/.html files which also introduces a potential stored XSS vector more if its rendered without sanitization.