Group no: 14

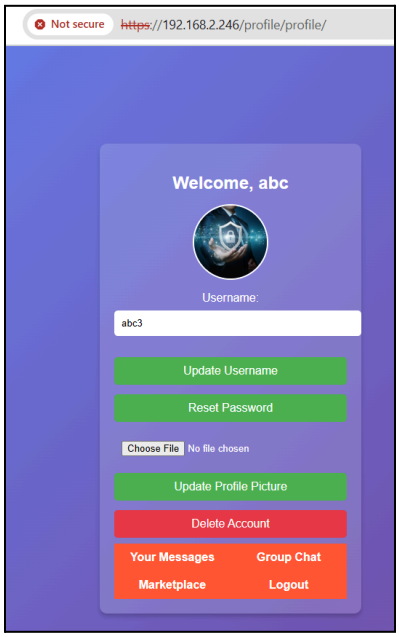
Vulnerability Type:
Security

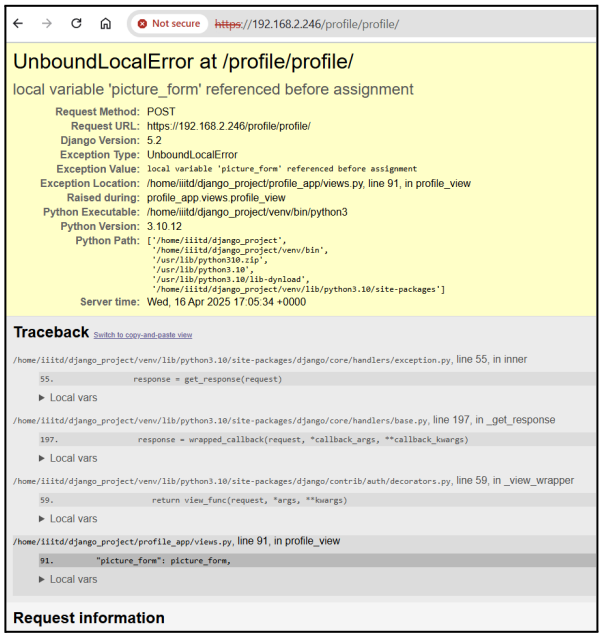
Brief Discription: The /profile/profile/ page gives an error when i try to change the username to one that already exists. This shows two main security problems: IDOR, where users can try to change other users' profiles, and Sensitive Information Exposure, as the error reveals backend details about how the website works behind the scenes including file paths, Python version, and internal variable names which could help attackers.

Steps to Reproduce:

1) Login as a existinguser or create a new user and login.
2) Go to https://192.168.2.246/profile/profile/
3) Update the username to a name that you know already exists.
4) Then see that that the server crashes and throws an UnboundLocalError. Also see the stack trace that is revealed in the browser along with paths and code details.

Proof of Concept: I logged in as abc1 and updated username to abc3 (which already exists) and the server returned the following error: UnboundLocalError at /profile/profile/
The traceback reveals internal paths: /home/iiitd/django_project/profile_app/views.py, Python 3.10, Django 5.2, line 91, variable names, etc.





Impact:
The UnboundLocalError due to unassigned variables may crash user sessions or cause service interruptions thus afeecting Availability. Also it can lead to IDOR attack as any logged-in user can attempt to overwrite or view other users' data without authorization, leading to potential account hijacking or unauthorized profile updates. Also revealing server-side code structure and error logs publicly in the UI can assist an attacker in discovering vulnerabilities and exploiting them more effectively.