

Group no: 3

Vulnerability Type:

Security

Description: In this sensitive user information like name, email, bio, ID, and even cryptographic keys (encrypted_private_key, public_key, salt, etc.) are exposed in the frontend in the network tab in inspect (ctrl+shift+i). This includes details of all users and not just the logged-in user.

Steps to Reproduce:

- 1) Go to: https://192.168.2.235/add_friend
- 2) Go to the network tab in inspect elements (ctrl+shift+i).
- 3) Now see this request: `users?page=1&limit=10`.
- 4) Click on this and in the response tab see that all the user data including PII and cryptographic info is exposed.

Proof of Concept: In this i checked the `users?page=1&limit=10` request and saw that all the user have their details like encrypted_private_key, salt, iv, etc viewable to any user of the system through a simple inspection of network traffic.

The top screenshot shows the 'Add Friends' page with a search bar and a list of users. The network tab shows a request to `users?page=1&limit=10` with a response containing user data. The bottom screenshot shows the same page with a search filter applied, displaying 'fsha' and 'fsha270'. The network tab shows a request to `users?page=1&limit=10` with a response containing user data.

Impact:

This is a high security and privacy vulnerability. Leaking cryptographic keys and private user information exposes all users to identity theft, impersonation, and potential cryptographic attacks. This is a serious violation of privacy and basic web security best practices.