■■ Vauju Dating Platform – Penetration Test Report

Tested by: Mandip Guragai a.k.a Lil Mafia
Date: October 2025
Scope: Authorized private pen-test for backend-vauju-1.onrender.com and vauju.vercel.app

■ Summary of Findings

The Vauju platform contains multiple critical vulnerabilities allowing full account manipulation without authentication. These are exploitable through zero-click, cross-origin methods with no user interaction required.

■ Vulnerabilities Identified

#	Title	Description
1	IDOR on Profile Update	PUT /api/profile uses X-User-Id header without auth. Any profile can be updated by
2	Message Spoofing via Conversation ID	Attacker can flip sender/victim ID in message requests to spoof chats.
3	Sensitive Info Disclosure	Message request leaks victim email, username, bio even when profile is not viewab
4	Zero-Click Account Control	Victim does not need to interact. Only the user ID is needed to manipulate accounts

■■ Recommendations

• **API Auth**: Enforce proper token validation (e.g., JWT). Never trust X-User-Id directly.
• **Access Control**: Ensure users can only access/update their own data via backend validation.
• **Messaging**: Lock down sender and conversation ID manipulation.
• **Profile Update**: Switch to PATCH, not PUT. Bind requests to verified user tokens.
• **Privacy**: Hide email, bio, and username unless made public by the user.
• **CSRF / CORS**: Implement CSRF tokens. Lock down CORS policies to same-origin.
• **Admin Protection**: Separate admin logic and enforce strict role-based checks.
• **Rate Limiting**: Apply brute-force protection to login and other sensitive endpoints.

■ Testing Completed. Developer re-test and patch verification recommended before release.