Extra Credit – This is a quick contract. Write a small paper listing all the vulnerabilities that could happen in this contract in case someone wants to hack it. This can also include vulnerabilities throughout the entire app.

Smart Contract Vulnerabilities

1. Incorrect Access Control – Functions not properly restricted to admin roles.
2. Use of tx.orgin – Makes the contract vulnerable to phishing-style attacks.
3. Weak Address Verification – Poor hashing or comparison logic can be spoofed.
4. No Event Logging – Makes it hard to track changes like adding admins.
5. Lack of Reentrancy Protection – If any Ether transfers are involved.

App-Level Vulnerabilities

1. Exposed Backend Wallet Key – Stored insecurely or hardcoded in the backend.
2. Unsecured API Route – Anyone could call the verify route if not protected.
3. Frontend Role Spoofing – Admin status shown via localStorage can be faked.
4. No HTTPS – Allows man-in-the-middle attacks on verification calls.
5. No Rate Limiting – Leaves the backend or contract open to spam/DoS attacks.